Migration, Installation und Konfiguration von ADOBE® ACROBAT® CONNECT™ PRO SERVER 7.5



Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Inhalt

Kapitel 1: Vorbereiten der Migration, Installation und Konfiguration

Lesen Sie die Abschnitte zu den Installationsanforderungen und den unterstützten Konfigurationen sowie den technischen Überblick, um sich auf den Entwurf und die Installation eines Adobe® Acrobat® Connect™ Pro Server 7.5-Systems vorzubereiten. Wenn Sie eine Aktualisierung auf Acrobat Connect Pro Server 7.5 durchführen, befolgen Sie die Anweisungen zur Sicherung von Dateien.

Neue Funktionen in Acrobat Connect Pro Server 7.5

Folgende Funktionen sind neu oder haben sich seit Acrobat Connect Pro Server 7.5 geändert:

VMWare Acrobat Connect Pro Server 7.5 fügt Unterstützung für die Installation in einer VMWare-Umgebung hinzu. Weitere Informationen finden Sie in der VMWare-Konfigurationsbeschreibung und den Connect Pro Server-Systemanforderungen.

Universal Voice Mit der Acrobat Connect Pro Server 7.5-Universal Voice-Lösung können Sie Audiokonferenzen über VoIP live an Meetingteilnehmer streamen. Sie können die Audiokonferenz des Connect Pro-Meetings auch live aufzeichnen.

Installieren und konfigurieren Sie zur Bereitstellung der Universal Voice-Lösung Adobe Flash Media Gateway zusammen mit der Acrobat Connect Pro Server 7.5-Installation. Flash Media Gateway ist fester Bestandteil des Acrobat Connect Pro Server 7.5-Installationsprogramms. Flash Media Gateway ermöglicht die Kommunikation zwischen Acrobat Connect Pro Server 7.5 und Ihrer SIP-Infrastruktur. Flash Media Gateway lässt sich auf demselben Server mit Acrobat Connect Pro Server 7.5 installieren oder auf einem anderen Computer. Weitere Informationen hierzu finden Sie unter „Bereitstellen von Universal Voice“ auf Seite 40.

Hinweis: *Zusätzlich zu Universal Voice bietet Acrobat Connect Pro Server 7.5 auch vollständig integrierte Telefonieadapter mit erweiterter Anrufsteuerung und komfortabler Teilnehmerrückmeldung. Weitere Informationen finden Sie unter* *„Audiokonferenzoptionen mit Connect Pro“ auf Seite 14.*

Freigeben von Adobe® PDF files Nutzen Sie PDF-Dateien in Ihren Meetingräumen gemeinsam. Wählen Sie in einem Meetingraum die gemeinsam zu nutzenden PDF-Dateien aus der Connect Pro Central-Inhaltebibliothek oder von Ihrem Computer aus. In der Inhaltsbibliothek werden PDF-Dateien als PDF-Dateien gespeichert. Zur Ansicht im Meetingraum werden die PDF-Dateien in SWF-Dateien konvertiert. Weitere Informationen finden Sie unter Dokumente gemeinsam nutzen.

Verbesserte Unterstützung für Microsoft® PowerPoint Geben Sie PPTX-Dokumente in Meetingräumen mit höherer Auflösung frei, einschließlich Dokumente mit Smart-Art, Diagrammen, Text- und Shape-Effekten. Moderatoren können PPTX-Dokumente in höherer Auflösung von Windows- oder Macintosh-Betriebssystemen in Meetingräume hochladen.

Adobe Acrobat Connect Pro-Add-In für IBM Lotus Notes Planen und verwalten Sie Adobe Acrobat Connect Pro-Meetings mit Lotus Notes. Weitere Informationen hierzu finden Sie unter Adobe Acrobat Connect Pro-Add-In für IBM Lotus Notes Installations- und Bereitstellungshandbuch und Verwenden des Adobe Acrobat Connect Pro-Add-Ins für IBM Lotus Notes.

Support- und Statusverknüpfungen im Hilfemenü des Meetingraums Fügen Sie dem Meetingraum-Hilfemenü über Konfigurationsparameter in der Datei "custom.ini" Support- und Statuselemente hinzu. Legen Sie URLs fest, über die Meetingteilnehmer Informationen über Hilfeoptionen und den Systemstatus abrufen können. Mit Acrobat Connect Pro-Webservices können Sie Seiten mit dynamischen Informationen über den Systemstatus erstellen. Weitere Informationen finden Sie unter „Hinzufügen von Support- und Statusverknüpfungen im Hilfemenü“ auf Seite 51.

Installationsanforderungen

Hardware-, Software- und Benutzeranforderungen

Weitere Informationen in Bezug auf die Anforderungen für Adobe Acrobat Connect Pro Server und Adobe Acrobat Connect Pro Edge Server finden Sie unter www.adobe.com/go/connect_sysreqs_de.

Portanforderungen

In der folgenden Tabelle sind die Ports aufgeführt, über die Benutzer in der Lage sein sollten, TCP-Verbindungen herzustellen.

Nummer	Bind-Adresse	Zugriff	Protokoll
80	*/Beliebiger Adapter	Öffentlich	HTTP, RTMP
443	*/Beliebiger Adapter	Öffentlich	HTTPS, RTMPS
1935	*/Beliebiger Adapter	Öffentlich	RTMP

Hinweis: *RTMP (Real-Time Messaging Protocol) ist ein Adobe-Protokoll.*

In der folgenden Tabelle werden die Ports beschrieben, die innerhalb eines Clusters offen sind. Jeder Acrobat Connect Pro-Server in einem Cluster muss über diese Ports TCP-Verbindungen zu allen anderen Servern im Cluster herstellen können.

Hinweis: *Diese Ports sollten nicht öffentlich zugänglich sein, auch wenn Sie keinen Cluster verwenden.*

Nummer	Quellport	Bind-Adresse	Zugriff	Protokoll
8506	Beliebig	*/Beliebiger Adapter	Privat	RTMP
8507	Beliebig	*/Beliebiger Adapter	Privat	HTTP

Jeder Acrobat Connect Pro-Server in einem Cluster muss über den folgenden Port eine TCP-Verbindung zum Datenbankserver herstellen können:

Nummer	Quellport	Zugriff	Protokoll
1433	Beliebig	Privat	TSQL

In der folgenden Tabelle sind die Serverports aufgeführt, die Acrobat Connect Pro für die interne Kommunikation verwendet. Diese Ports dürfen auf einem Server, der Acrobat Connect Pro hostet, nicht verwendet werden; andernfalls kann Acrobat Connect Pro nicht gestartet werden.

Nummer	Bind-Adresse	Zugriff	Protokoll
1111	127.0.0.1	Intern	RTMP
1434	127.0.0.1 Dieser Port ist nur dann aktiv, wenn Sie die eingebettete Datenbank verwenden.	Intern	TSQL
2909	127.0.0.1	Intern	RMI
4111	*/Beliebiger Adapter	Intern	JMX
8510	127.0.0.1	Intern	HTTP

Weitere Informationen über Flash Media Gateway-Ports finden Sie unter „Flash Media Gateway-Ports und -Protokolle“ auf Seite 42.

Unterstützte Konfigurationen

Unterstützte Server-/Datenbankkonfigurationen

Acrobat Connect Pro verwendet eine Datenbank zum Speichern von Informationen über Benutzer und Materialien. Im Folgenden werden die unterstützten Datenbank- und Acrobat Connect Pro-Konfigurationen aufgelistet:

Einzelner Server mit eingebetteter Datenbank-Engine Acrobat Connect Pro wird auf einem einzelnen Computer installiert, auf dem auch die eingebettete Datenbank-Engine (im Installationsprogramm von Acrobat Connect Pro enthalten) installiert wird. Die eingebettete Datenbank-Engine ist Microsoft® SQL Server® 2005 Express Edition.

***Hinweis:** Diese Konfiguration sollte nur in Testumgebungen, nicht in Produktionsumgebungen verwendet werden.*

Einfacher Server mit SQL Server 2005 Standard Edition-Datenbank Installieren Sie Acrobat Connect Pro auf einem einzelnen Computer und installieren Sie Microsoft® SQL Server 2005 Standard Edition auf demselben Computer.

Einzelner Server mit externer SQL Server 2005 Standard Edition-Datenbanken Installieren Sie Acrobat Connect Pro auf einem einzelnen Computer und installieren Sie auf einem anderen Computer SQL Server 2005 Standard Edition.

Einzelner Server mit mehreren externen SQL Server 2005 Standard Edition-Datenbank Installieren Sie Acrobat Connect Pro auf einem einzelnen Computer und installieren Sie SQL Server 2005 Standard Edition auf mehreren Computern (auch „Cluster“ genannt) außerhalb von Acrobat Connect Pro. Acrobat Connect Pro unterstützt das Spiegeln und den Clusterbetrieb von SQL Server-Datenbanken.

Mehrere Server mit externer SQL Server 2005 Standard Edition-Datenbank Installieren Sie Acrobat Connect Pro auf mehreren Computern (auch „Cluster“ genannt) und installieren Sie SQL Server 2005 Standard Edition auf einem anderen Computer.

Mehrere Server mit mehreren externen SQL Server 2005 Standard Edition-Datenbanken Installieren Sie Acrobat Connect Pro auf mehreren Computern (auch „Cluster“ genannt) und installieren Sie SQL Server 2005 Standard Edition in einem separaten Cluster. Acrobat Connect Pro unterstützt das Spiegeln und den Clusterbetrieb von SQL Server-Datenbanken.

***Hinweis:** Microsoft SQL Server Standard Edition ist nicht im Lieferumfang von Acrobat Connect Pro Server 7.5 enthalten, sondern muss separat erworben werden.*

Verwandte Themen

„Vorbereiten der Installation“ auf Seite 7

„Installieren von Connect Pro Server und Flash Media Gateway“ auf Seite 16

Unterstützte Flash Media Gateway-Bereitstellungsarten

Stellen Sie Flash Media Gateway bereit, um Universal Voice zu aktivieren. Folgende Bereitstellungsarten werden unterstützt:

Einzelner Computer Installieren Sie Connect Pro Server, Flash Media Gateway und SQL-Server auf demselben Computer.

Zwei Computer Installieren Sie Connect Pro Server und Flash Media Gateway auf demselben Computer und SQL Server auf einem separaten Computer.

Computercluster Installieren Sie die einzelnen Connect Pro Server- und Flash Media Gateway-Instanzen auf separaten Computern.

Verwandte Themen

„Audiokonferenzoptionen mit Connect Pro“ auf Seite 14

„Bereitstellen von Universal Voice“ auf Seite 40

Unterstützte LDAP-Verzeichnisserver

Sie können in der Konfiguration festlegen, dass Benutzer anhand des LDAP-Verzeichnisservers Ihres Unternehmens authentifiziert werden und Verzeichnisinformationen direkt vom LDAP-Verzeichnisservers Ihres Unternehmens in Acrobat Connect Pro importieren. Eine Liste der unterstützten LDAP-Verzeichnisserver finden Sie unter www.adobe.com/go/connect_sysreqs_de.

Hinweis: *Acrobat Connect Pro Server 7.5 lässt sich mit einem beliebigen LDAP v.3 Directory-Server zusammen betreiben. Allerdings werden nur Directory-Server unterstützt, die von Adobe getestet wurden.*

Verwandte Themen

„Integration mit einem Verzeichnisdienst“ auf Seite 32

Unterstützte Materialspeichergeräte

Sie können das Acrobat Connect Pro-System so konfigurieren, dass Materialien auf NAS-Geräten (Network Attached Storage) oder auf SAN-Geräten (Storage Area Network) gespeichert werden können. Eine Liste der unterstützten NAS- und SAN-Geräte finden Sie unter www.adobe.com/go/connect_sysreqs_de.

Verwandte Themen

„Konfigurieren von gemeinsamem Speicher“ auf Seite 48

Vorbereitung der Migration

Migrationspfade

Starten Sie das Adobe Acrobat Connect Pro Server 7.5-Installationsprogramm, um ein Upgrade von Adobe Connect Pro Server 7.x auf Acrobat Connect Pro Server 7.5 durchzuführen. Dies ist der einzige Upgrade-Pfad. Das Installationsprogramm für Acrobat Connect Pro Server und die Anwendungsverwaltungskonsole bieten grafische Benutzeroberflächen, die Sie Schritt für Schritt durch ein Upgrade führen.

Weitere Upgrade-Informationen erhalten Sie vom technischen Support von Adobe: www.adobe.com/go/connect_licensed_programs_de.

Migrieren von Acrobat Connect Pro Server 7.x auf Acrobat Connect Pro Server 7.5

Folgen Sie diesem Arbeitsablauf, um Acrobat Connect Pro Server 7.x auf Acrobat Connect Pro Server 7.5 zu migrieren.

1. Testen Sie die Migration in einer Testumgebung (keine Produktionsumgebung).

Vor der Migration der Produktionsumgebung empfiehlt es sich, einen Schnappschuss der aktuellen Produktionsumgebung zu erstellen und die Migration zunächst in einer Testumgebung durchzuführen. Wenn die Migration der Testumgebung erfolgreich war, fahren Sie mit Schritt 2 fort.

2. Informieren Sie die Benutzer über die Migration.

Weitere Informationen finden Sie unter „Informieren der Benutzer über die Migration“ auf Seite 6.

3. (Optional) Sichern Sie Inhalte und Konfigurationsdateien.

Weitere Informationen finden Sie unter „Sichern von Dateien“ auf Seite 6.

4. Erstellen Sie eine Sicherungskopie der Datenbank.

Weitere Informationen finden Sie unter „Sichern der Datenbank“ auf Seite 105.

5. Starten Sie das Adobe Acrobat Connect Pro Server 7.5-Installationsprogramm.

Weitere Informationen hierzu finden Sie unter „Installieren von Connect Pro Server und Flash Media Gateway“ auf Seite 16. Das Installationsprogramm beendet die Acrobat Connect Pro Server-Dienste und sichert bestehende Dateien, einschließlich der "custom.ini"-Datei.

6. Konfigurieren Sie Acrobat Connect Pro Server 7.5

Weitere Informationen hierzu finden Sie unter „Konfigurieren von Acrobat Connect Pro mit dem Assistenten der Anwendungsverwaltungskonsole“ auf Seite 18.

7. Überprüfen Sie die Installation.

Weitere Informationen finden Sie unter „Überprüfen der Installation“ auf Seite 20.

Informieren der Benutzer über die Migration

Bei jedem Software-Upgrade sind Kommunikation und Planung von entscheidender Bedeutung, insbesondere dann, wenn eine Arbeitsgruppe betroffen ist. Bevor Sie mit der Migration oder mit dem Hinzufügen von Modulen zu Acrobat Connect Pro beginnen, sollten Sie folgende Schritte ausführen:

- Planen Sie ausreichend Zeit für die Migration ein. Das Upgrade sollte während der regulären Wartungszeit stattfinden.
- Informieren Sie die Benutzer im Voraus, dass Acrobat Connect Pro während der Migration nicht zur Verfügung stehen wird.
- Teilen Sie den Benutzern mit, welche Änderungen nach der Migration zu erwarten sind (wie neue Funktionen oder höhere Leistung). Informationen über neue Funktionen finden Sie unter www.adobe.com/go/learn_cnn_whatsnew_de.

Sichern von Dateien

Das Installationsprogramm erstellt Sicherungskopien der Verzeichnisse „appserv“ und „comserv“ sowie der Datei „custom.ini“ und installiert neue Versionen. Das Installationsprogramm löscht oder überschreibt nicht das Verzeichnis „content“.

Optional können Sie auch das Erstellen von Sicherungskopien dieser Verzeichnisse und Dateien auswählen.

Aktualisieren von SQL Server 2005 Express Edition

Im Folgenden wird beschrieben, wie Sie eine Migration von der eingebetteten Datenbank auf SQL Server zur Verwendung auf einem anderen Computer durchführen.

Hinweis: *Diese Migration lässt sich beim Migrieren von Acrobat Connect Pro Server 7.x auf Acrobat Connect Pro Server 7.5. durchführen, oder zu einem beliebigen Zeitpunkt nach der Installation von Acrobat Connect Pro Server 7.5.*

1. Installieren von SQL Server 2005 Standar Edition auf einem Computer, der nicht zugleich Connect Pro Server ausführt

Folgen Sie den Microsoft-Anleitungen zur Installation von SQL Server.

2. Sichern von SQL Server 2005 Express Edition

Weitere Informationen finden Sie unter „Sichern der Datenbank“ auf Seite 105.

3. Kopieren der.bak-Datei vom Connect Pro Server-Host-Computer auf den SQL Server-Host-Computer.

Wenn Sie eine Sicherungskopie von SQL Server Express Edition erstellen, wird eine Datei namens „*breeze*.bak“ erstellt (dabei ist *breeze* der Name der Datenbank).

4. Wiederherstellen der Datenbank auf dem Server, der als Host für SQL Server 2005 Standard Edition dient.

Weitere Informationen zum Wiederherstellen von SQL Server finden Sie im Microsoft TechNet.

5. Eingeben der Datenbankinformationen für SQL Server 2005 Standard Edition in der Anwendungsverwaltungskonsole des Servers, der als Host für Connect Pro dient.

Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server “ > „Adobe Acrobat Connect Pro Server 7 konfigurieren“.

Vorbereiten der Installation

Technische Informationen zu Acrobat Connect Pro

Eine Acrobat Connect Pro-Installation besteht aus mehreren Komponenten: Connect Pro Central Application Server, Adobe® Flash® Media Server, Connect Pro Presence Service, Flash Media Gateway und einer Datenbank.

Connect Pro Central Application Server stützt sich auf J2EE und verwendet Komponenten von Macromedia® JRun™ von Adobe. Diese Komponente wird auch als *Anwendungsserver* bezeichnet und verwaltet Benutzer, Gruppen, On-Demand-Materialien und Clientsitzungen. Zu den Aufgaben des Anwendungsservers gehören Zugriffssteuerung, Sicherheit, Kontingente, Lizenzierung sowie Auditing- und Verwaltungsfunktionen wie Clustering, Ausfallsicherung und Replikation. Er ist auch für die Umwandlung von Medien zuständig, beispielsweise für die Konvertierung von Microsoft® PowerPoint und Audiomaterial in Adobe® Flash®. Der Anwendungsserver verarbeitet Meetinganfragen und Materialübertragungsanforderungen (Folien, HTTP-Seiten, SWF-Dateien und Dateien im Dateifreigabe-Pod) über eine HTTP- oder HTTPS-Verbindung.

Flash Media Server, auch *Meetingserver* genannt, wird mit Acrobat Connect Pro installiert und ist für das Audio- und Video-Streaming in Echtzeit, die Datensynchronisation sowie die Bereitstellung von Rich-Media-Material zuständig, darunter auch für die Interaktion mit Acrobat Connect Pro. Zu den Aufgaben von Flash Media Server gehört die Aufzeichnung und Wiedergabe von Meetings, die Synchronisation von Audio und Video und das Transcoding, d. h. die Konvertierung und Komprimierung von Daten für die Bildschirmfreigabe und Interaktion in Echtzeit. Flash Media Server reduziert die Serverlast und die Wartezeiten, indem häufig aufgerufene Webseiten, Streams und freigegebene Daten im Cache gespeichert werden. Flash Media Server verwendet zum Streaming von Audio, Video und zugehörigen Meetingdaten das leistungsfähige Real Time Messaging Protocol von Adobe (RTMP oder RTMPS).

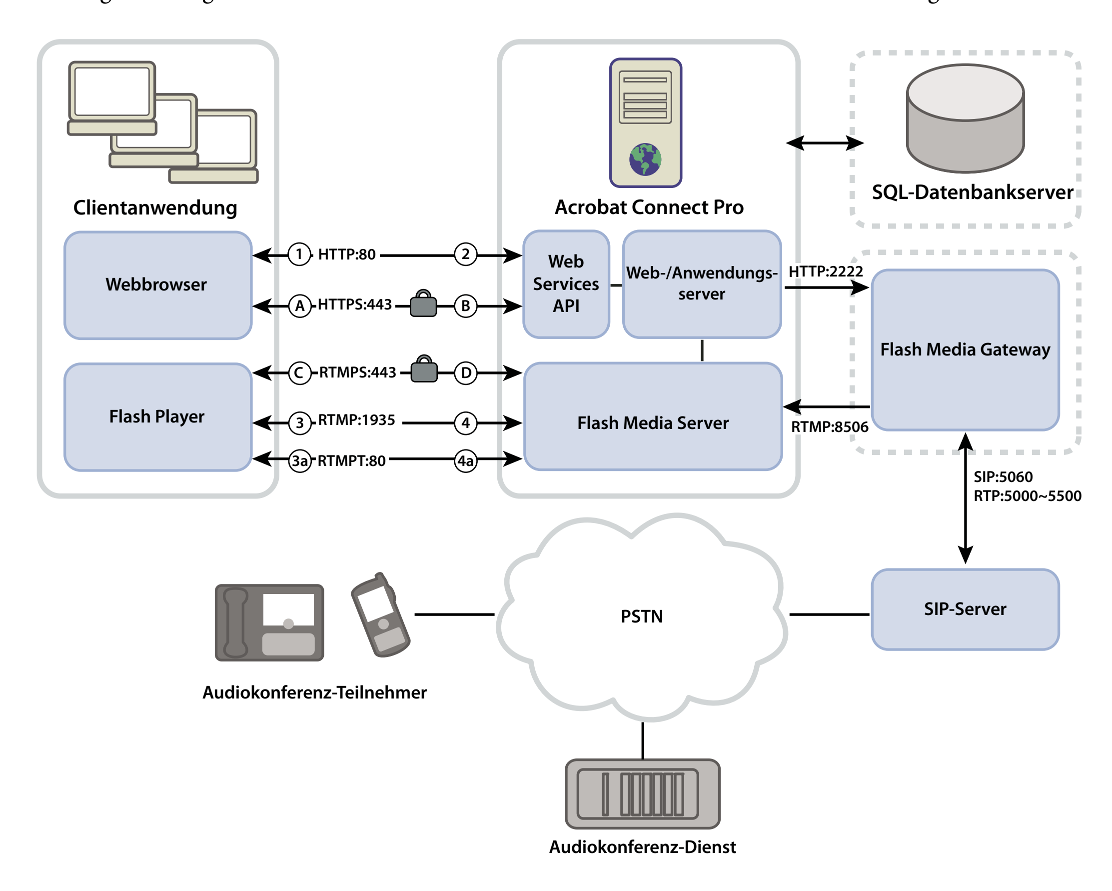
Connect Pro Presence Service integriert Acrobat Connect Pro mit Microsoft® Live Communication Server 2005 und Microsoft® Office Communication Server, um ihre IM-Präsenz in Meetingräumen von Acrobat Connect Pro anzeigen zu können.

Flash Media Gateway integriert Acrobat Connect Pro in Ihre SIP/RTP-Infrastruktur. Flash Media Gateway bezieht Audiodaten von einem SIP-Server und sendet sie an Connect Pro-Meetingräume. Diese Lösung heißt Universal Voice.

Acrobat Connect Pro erfordert eine Datenbank zum permanenten Speichern von transaktions- und anwendungsspezifischen Metadaten, einschließlich Informationen zu Benutzern, Gruppen, Materialien und Berichten. Sie können entweder das eingebettete Datenbank-Engine (SQL Server 2005 Express Edition) als Teil des Acrobat Connect Pro Server 7.5-Installationsprogramms nutzen, oder eine Lizenz für Microsoft SQL Server 2005 Standard Edition erwerben und dieses Produkt installieren.

Datenfluss

Das folgende Diagramm veranschaulicht den Datenfluss zwischen einer Clientanwendung und Acrobat Connect Pro.



Die Daten können über eine unverschlüsselte Verbindung oder über eine verschlüsselte Verbindung übertragen werden.

Unverschlüsselte Verbindung

Unverschlüsselte Verbindungen werden über HTTP und RTMP hergestellt und folgen dem in der Tabelle beschriebenen Pfad. Die Zahlen in der Tabelle entsprechen den Zahlen im Datenflussdiagramm.

Nummer	Beschreibung
2	Der Client-Webbrowser fordert über HTTP 80 eine Meeting- oder Material-URL an.
2	Der Webserver antwortet und überträgt das Material oder sendet dem Client Informationen zur Verbindung mit dem Meeting.
3	Der Flash Player des Clients fordert über RTMP:1935 eine Verbindung zum Meeting an.
3a	Der Flash Player des Clients fordert eine Verbindung zum Meeting an, kann aber nur RTMP:80 verwenden.
4	Flash Media Server antwortet und öffnet eine dauerhafte Verbindung für Acrobat Connect-Streaming-Verkehr.
4a	Flash Media Server antwortet und öffnet eine getunnelte Verbindung für Acrobat Connect-Streaming-Verkehr.

Verschlüsselte Verbindung

Verschlüsselte Verbindungen werden über HTTPS und RTMPS hergestellt und folgen dem in der Tabelle beschriebenen Pfad. Die Buchstaben in der Tabelle entsprechen den Buchstaben im Datenflussdiagramm.

Buchstabe	Beschreibung
A	Der Client-Webbrowser fordert über eine sichere Verbindung an HTTP:443 eine Meeting- oder Material-URL an.
B	Der Webserver antwortet und überträgt das Material über eine sichere Verbindung oder sendet dem Client Informationen zur sicheren Verbindung mit dem Meeting.
C	Der Flash Player des Clients fordert eine sichere Verbindung zu Flash Media Server über RTMPS:443 an.
D	Flash Media Server antwortet und öffnet eine sichere, dauerhafte Verbindung für Acrobat Connect Pro-Streaming-Verkehr.

Arbeitsablauf bei der Installation

In den folgenden Schritten wird beschrieben, wie Sie ein Acrobat Connect Pro-System entwerfen, installieren und konfigurieren. Bei einigen Schritten müssen Sie eine Entscheidung treffen, bei anderen eine bestimmte Aufgabe ausführen. In jedem Schritt wird auf Hintergrundinformationen zur Entscheidung oder Aufgabe verwiesen.

1. Wählen Sie die gewünschte Datenbank aus.

Weitere Informationen finden Sie unter „Auswählen einer Datenbank“ auf Seite 11.

2. Installieren Sie Acrobat Connect Pro auf einem Server.

Weitere Informationen hierzu finden Sie unter „Installieren von Connect Pro Server und Flash Media Gateway“ auf Seite 16. Wenn Sie in Schritt 1 die eingebettete Datenbank-Engine ausgewählt haben, müssen Sie sie ebenfalls installieren. Die eingebettete Datenbank-Engine ist Teil des Installationsprogramms von Acrobat Connect Pro.

3. Wenn Sie in Schritt 1 SQL Server 2005 Standard Edition ausgewählt haben, installieren Sie diese Komponente.

Weitere Informationen finden Sie in der Dokumentation zu SQL Server.

4. Stellen Sie Acrobat Connect Pro bereit.

Weitere Informationen finden Sie unter „Bereitstellen von Acrobat Connect Pro Server“ auf Seite 25.

5. Überprüfen Sie, ob Acrobat Connect Pro richtig installiert wurde.

Weitere Informationen finden Sie unter „Überprüfen der Installation“ auf Seite 20.

6. (Optional) Integrieren Sie Acrobat Connect Pro in Ihre Infrastruktur.

Zur Integration von Acrobat Connect Pro in die vorhandene Unternehmensinfrastruktur gibt es zahlreiche Möglichkeiten. Es empfiehlt sich, nach der Konfiguration einer jeden Komponente die Funktionsfähigkeit von Acrobat Connect Pro zu überprüfen.

In ein SIP-Gateway integrieren Integrieren Sie für nahtlose Audiokonferenzen Acrobat Connect Pro mit dem SIP-Anbieter (auch *VoIP-Anbieter* genannt) Ihres Unternehmens integrieren. Weitere Informationen hierzu finden Sie unter „Bereitstellen von Universal Voice“ auf Seite 40.

In ein LDAP-Verzeichnis integrieren Integrieren Sie Acrobat Connect Pro in den LDAP-Verzeichnisserver Ihres Unternehmens, damit Sie nicht mehrere Benutzerverzeichnisse verwalten müssen. Weitere Informationen finden Sie unter „Integration mit einem Verzeichnisdienst“ auf Seite 32.

Secure Socket Layer konfigurieren Die gesamte Kommunikation mit Acrobat Connect Pro sollte auf sichere Weise erfolgen. Weitere Informationen hierzu finden Sie unter „SSL (Secure Sockets Layer)“ auf Seite 68.

Material auf NAS/SAN-Geräten speichern Verwenden Sie Netzwerkgeräte, um den Speicheraufwand für Material zu verteilen. Weitere Informationen finden Sie unter „Konfigurieren von gemeinsamem Speicher“ auf Seite 48.

In Live Communication Server und Office Communication Server integrieren Integrieren Sie Connect Pro in einem Kommunikationsserver, um Meetingveranstaltern die Möglichkeit zu geben, die IM-Präsenz von eingeladenen Personen in Meetingräumen zu sehen. Meetingveranstalter können an IM-Benutzer vom Meetingraum aus auch Nachrichten senden. Weitere Informationen finden Sie unter „Integrieren mit Microsoft Live Communications Server 2005 und Microsoft Office Communications Server 2007“ auf Seite 54.

Public-Key-Infrastruktur konfigurieren Wenn Sie Acrobat Connect Pro in einen LDAP-Verzeichnisserver integriert haben, können Sie eine zusätzliche Sicherheitsstufe einrichten, indem Sie vorgeben, dass Client-Zertifikate erforderlich sind. Weitere Informationen finden Sie unter „PKI (Public Key-Infrastruktur)“ auf Seite 82.

Hosting für Acrobat Connect-Add-In einrichten Die Benutzer können das Add-In für Acrobat Connect ganz einfach von Adobe-Servern herunterladen. Wenn die Sicherheitsmaßnahmen Ihres Unternehmens jedoch keine externen Downloads zulassen, können Sie einen eigenen Server als Host für das Add-In verwenden, ohne dass dies für Benutzer mit Nachteilen verbunden ist. Weitere Informationen finden Sie unter „Hosting für Acrobat Connect-Add-In“ auf Seite 66.

7. (Optional) Legen Sie fest, ob Acrobat Connect Pro Server 7.5 in einem Cluster installiert werden soll.

Weitere Informationen finden Sie unter „Entscheidung für die Bereitstellung von Acrobat Connect Pro in einem Cluster“ auf Seite 10 und „Bereitstellen eines Clusters aus Acrobat Connect Pro-Servern“ auf Seite 25.

8. (Optional) Legen Sie fest, ob Edge-Server installiert werden sollen.

Weitere Informationen hierzu finden Sie unter „Auswahl der Bereitstellung von Acrobat Connect Pro Edge Server“ auf Seite 12 und „Bereitstellen von Acrobat Connect Pro Edge Server“ auf Seite 30.

Entscheidung für die Bereitstellung von Acrobat Connect Pro in einem Cluster

Es ist zwar möglich, alle Komponenten von Acrobat Connect Pro Server , einschließlich der Datenbank, auf einem einzelnen Server zu installieren, doch wird diese Konfiguration nur für Testzwecke empfohlen, nicht aber für Produktionsumgebungen.

Eine Gruppe von verbundenen Servern, die alle für dieselbe Aufgabe zuständig sind, wird normalerweise als *Cluster* bezeichnet. Bei einem Acrobat Connect Pro Server -Cluster wird dieselbe Acrobat Connect Pro Server -Kopie auf jedem Server im Cluster installiert.

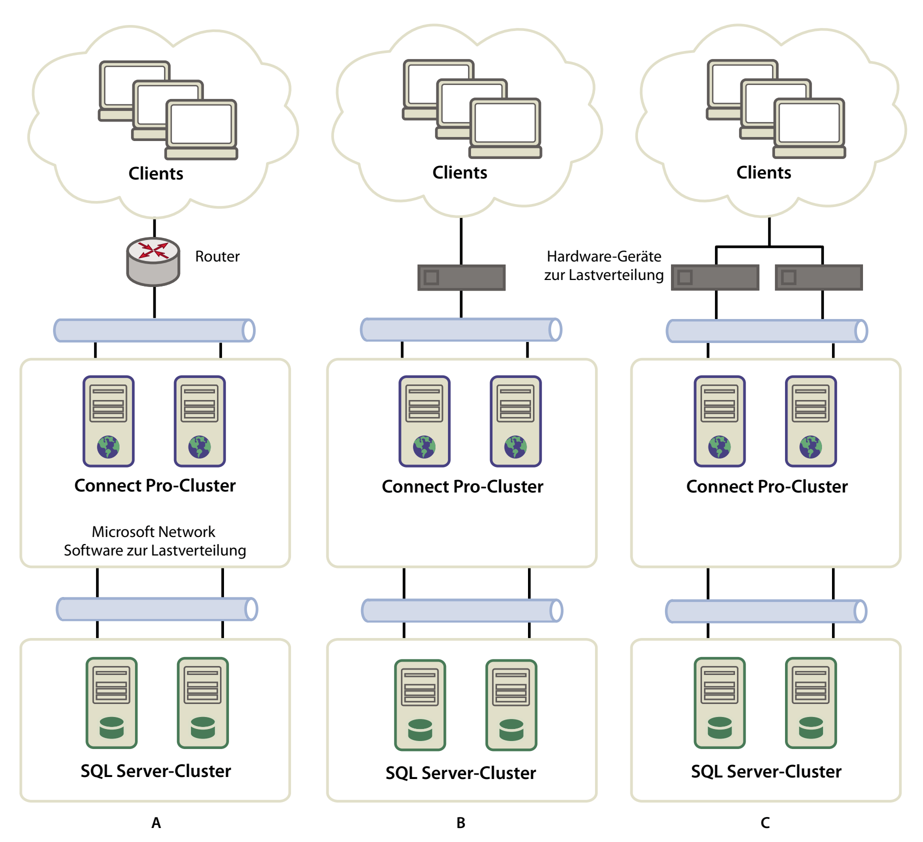
Hinweis: *Wenn Sie Acrobat Connect Pro Server in einem Cluster installieren, müssen Sie SQL Server 2005 Standard Edition verwenden und diese auf einem separaten Computer installieren.*

Fällt ein Host im Cluster aus, kann ein anderer Host im Cluster dessen Rolle übernehmen und dasselbe Meeting bereitstellen. Sie müssen Hardware oder Software von anderen Herstellern verwenden, um im Cluster für Lastausgleich zu sorgen. Häufig kann Hardware für den Lastausgleich auch als SSL-Beschleuniger eingesetzt werden.

Hinweis: *In der Anwendungsverwaltungskonsole können Sie gemeinsamen Speicher konfigurieren, sodass Material auf externen Geräten gespeichert und in Acrobat Connect Pro Server zwischengespeichert wird.*

Zuverlässige Netzwerksysteme verfügen über redundante Komponenten, das heißt, dass bei einem Ausfall einer Komponente eine andere, identische (*redundante*) Komponente die Aufgabe der ausgefallenen Komponente übernehmen kann. Wenn eine Komponente ausfällt und die redundante Komponente einspringt, erfolgt eine *Ausfallsicherung (Failover)*.

Im Idealfall sollte nicht nur Acrobat Connect Pro Server, sondern jede Komponente in einem System redundant sein. Möglich wäre beispielsweise der Einsatz von mehreren Hardwaregeräten für den Lastausgleich (wie BIG-IP von F5 Networks), einem Cluster aus Servern, die Acrobat Connect Pro Server hosten, und SQL Server-Datenbanken auf mehreren externen Computern. Erstellen Sie Ihr System mit einem Höchstmaß an Redundanz und sorgen Sie für einen kontinuierlichen Ausbau im Zeitverlauf.



Drei Optionen für die Anordnung in Clustern
A. *Ein Cluster mit Network Load Balancing-Software und zwei externen Datenbanken* ***B.*** *BIG-IP-Load-Balancing-Hardware, Cluster und zwei externe Datenbanken* ***C.*** *Zwei BIG-IP-Load-Balancing-Geräte, Cluster und zwei externe Datenbanken*

Verwandte Themen

„Bereitstellen eines Clusters aus Acrobat Connect Pro-Servern“ auf Seite 25

„Konfigurieren von gemeinsamem Speicher“ auf Seite 48

Auswählen einer Datenbank

Acrobat Connect Pro Server verwendet eine Datenbank zum Speichern von Informationen über Benutzer, Materialien, Kurse, Meetings und Berichte. Sie können entweder die eingebettete Datenbank-Engine verwenden (im Installationsprogramm enthalten) oder Microsoft SQL Server 2005 Standard Edition installieren (muss separat erworben werden).

Hinweis: *Die eingebettete Datenbank-Engine ist Microsoft SQL Server 2005 Express Edition.*

Eingebettete Datenbank

Die eingebettete Datenbank-Engine wird für Tests und Entwicklung empfohlen. Sie verwendet dieselben Datenstrukturen wie SQL Server 2005 Standard Edition, ist aber nicht so robust.

Die eingebettete Datenbank-Engine unterliegt den folgenden Einschränkungen:

- Die eingebettete Datenbank-Engine muss aus lizenzrechtlichen Gründen auf dem Computer installiert werden, auf dem auch Acrobat Connect Pro Server installiert ist. Der Computer darf nur einen Prozessor enthalten.
- Die Datenbank hat eine Maximalgröße von 2 GB.
- Die eingebettete Datenbank-Engine verfügt über eine Befehlszeilenoberfläche anstatt einer grafischen Benutzeroberfläche.

Microsoft SQL Server 2005 Standard Edition

Für Produktionsumgebungen wird Microsoft SQL Server 2005 Standard Edition empfohlen, da diese ein skalierbares Datenbankmanagementsystem (DBMS) ist, das zahlreiche Benutzer gleichzeitig unterstützen kann. SQL Server 2005 Standard Edition bietet auch eine grafische Benutzeroberfläche für Verwaltung und Abfrage der Datenbank.

SQL Server 2005 Standard Edition kann auf demselben Computer wie Acrobat Connect Pro Server oder auf einem anderen Computer installiert werden. Bei der Installation auf verschiedenen Computern müssen diese Computer mit derselben Zeitquelle synchronisiert werden. Weitere Informationen finden Sie in der folgenden TechNote: www.adobe.com/go/2e86ea67.

Installieren Sie SQL Server im gemischten Anmeldemodus, damit die SQL-Authentifizierung verwendet werden kann. Stellen Sie die Datenbank so ein, dass zwischen Groß- und Kleinschreibung unterschieden wird.

SQL Server muss in den folgenden Bereitstellungsszenarien verwendet werden:

- Die Datenbank soll auf einem Computer installiert werden, auf dem Acrobat Connect Pro Server nicht installiert ist.
- Acrobat Connect Pro Server ist in einem Cluster installiert.
- Acrobat Connect Pro Server ist auf Computern mit mehreren Prozessoren und Hyper-Threading-Technologie installiert.

Verwandte Themen

„Unterstützte Server-/Datenbankkonfigurationen“ auf Seite 3

„Installieren von Connect Pro Server und Flash Media Gateway“ auf Seite 16

Auswahl der Bereitstellung von Acrobat Connect Pro Edge Server

Wenn Sie Acrobat Connect Edge Server in Ihrem Netzwerk bereitstellen, erstellen Clients eine Verbindung mit dem Edge-Server und der Edge-Server erstellt eine Verbindung mit Acrobat Connect Pro (auch *Ursprungsserver* genannt). Diese Verbindungen erfolgen transparent – die Benutzer haben deshalb den Eindruck, dass sie direkt mit dem Ursprungsserver verbunden sind, auf dem das Meeting stattfindet.

Edge-Server bieten die folgenden Vorteile:

Kürzere Wartezeiten im Netzwerk Edge-Server bieten einen Zwischenspeicher für On-Demand-Material (wie aufgezeichnete Meetings und Präsentationen) und teilen Live-Streams, sodass der Netzwerkverkehr zum Ursprung geringer ist. Edge-Server platzieren Ressourcen in geringerer Entfernung zu den Clients.

Sicherheit Edge-Server bilden eine zusätzliche Schicht zwischen der Client-Internetverbindung und dem Ursprung.

Sofern dies im Rahmen Ihrer Lizenz zulässig ist, können Sie einen Cluster aus Edge-Servern installieren und konfigurieren. Das Implementieren der Edge-Server in einem Cluster bietet die folgenden Vorteile:

Ausfallsicherung Wenn ein Edge-Server ausfällt, werden die Clients an einen anderen Edge-Server umgeleitet.

Unterstützung für große Veranstaltungen Wenn für ein Meeting mehr als 500 Verbindungen gleichzeitig erforderlich sind, bietet ein einzelner Edge-Server nicht genügend Sockets. Ein Cluster ermöglicht mehr Verbindungen mit demselben Meeting.

Lastausgleich Wenn mehr als 100 Meetings gleichzeitig erforderlich sind, bietet ein einzelner Edge-Server möglicherweise nicht genug Arbeitsspeicher. Edge-Server können in einem Cluster hinter einem Lastausgleichmechanismus angeordnet werden.

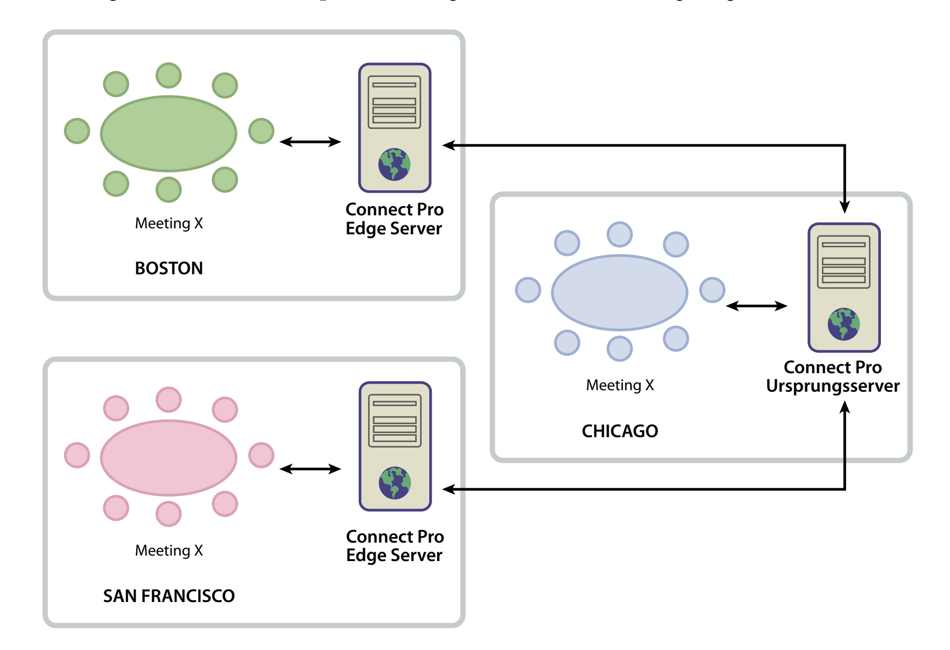
Funktionsweise von Edge-Servern

Edge-Server authentifizieren Benutzer und authentifizieren Ihre Anforderungen zum Zugriff auf Webdienste wie Acrobat Connect Pro Meeting, statt jede Anforderung an den Ursprungsserver weiterzuleiten und dessen Ressourcen mit diesen Aufgaben zu erschöpfen. Wenn die angeforderten Daten im Cache des Edge-Servers gefunden werden, gibt der die Daten an den anfordernden Client zurück, ohne Acrobat Connect Pro aufzurufen.

Wenn die angeforderten Daten nicht im Cache des Edge-Servers gefunden werden, gibt der Server die Anforderung des Clients an den Ursprungsserver weiter. Dort wird der Benutzer authentifiziert und die Dienstanforderung wird autorisiert. Der Ursprungsserver gibt die Ergebnisse an den anfordernden Edge-Server zurück, der seinerseits die Ergebnisse an den anfordernden Client übergibt. Der Edge-Server speichert diese Daten außerdem in seinem Cache, in dem andere authentifizierte Benutzer darauf zugreifen können.

Beispiel einer Edge-Server-Installation

Im Folgenden wird ein Beispiel einer Edge-Server-Installation gezeigt:



Die Clients am Standort Chicago verwenden den Ursprungsserver in einem Datencenter in Chicago. Die Edge-Server in Boston und San Francisco erfassen Anforderungen der lokalen Clients und leiten sie an den Ursprungsserver weiter. Die Edge-Server erhalten die Antworten vom Ursprungsserver in Chicago und leiten sie an die Clients in ihren Zonen weiter.

Verwandte Themen

„Installieren von Acrobat Connect Pro Edge Server“ auf Seite 22

„Bereitstellen von Acrobat Connect Pro Edge Server“ auf Seite 29

Erstellen und Optimieren einer VMWare-Umgebung

Die Installation von Connect Pro Server auf VMWare unterscheidet sich nicht von der Installation auf einem physischen Computer. Weitere Informationen über Hardware-, Software- und Konfigurationsanforderungen finden Sie im Whitepaper über das Ausführen von Connect Pro Server in einer virtuellen Umgebung.

Audiokonferenzoptionen mit Connect Pro

Connect Pro unterstützt zwei Möglichkeiten für die Verbindung mit Audiokonferenzanbietern: Universal Voice und integrierte Telefonieadapter. Beide Lösungen haben spezifische Vorteile. Für einen einzelnen Audioanbieter können Sie sowohl eine der beiden Lösungen als auch beide konfigurieren. Für ein Connect Pro-Konto lassen sich beliebig viele Audiokonferenzanbieter konfigurieren.

Universal Voice ermöglicht es Connect Pro, Audioübertragungen von beliebigen Audiokonferenzanbietern zu empfangen. Sie können das Audiomaterial zusammen mit der Webkonferenz aufzeichnen und es an Teilnehmer streamen, die nur über VoIP verbunden sind.

Die Lösung über Universal Voice verwendet die Komponente Flash Media Gateway, die mit Connect Pro Server zusammen installiert wird. Flash Media Gateway bezieht Audiodaten von einem SIP-Server und sendet sie über RTMP an Connect Pro-Meetingräume. Um Universal Voice nutzen zu können, müssen Sie entweder Ihren eigenen SIP-Server hosten oder ein entsprechendes Konto bei einem SIP-Anbieter besitzen. Weitere Informationen über das Konfigurieren von Flash Media Gateway finden Sie unter „Bereitstellen von Universal Voice“ auf Seite 40.

Nach der Bereitstellung von Universal Voice können Kontoadministratoren mit Connect Pro Central die Audiokonferenzinformationen konfigurieren. Weitere Informationen hierzu finden Sie unter www.adobe.com/go/learn_cnn_uvconfig_de.

Integrierte Telefonieadapter sind Java-Erweiterungen, mit denen die Kommunikation zwischen Connect Pro und speziellen Audiokonferenzanbietern ermöglicht wird. Integrierte Telefonieadapter bieten eine erweiterte Anrufsteuerung. Adobe stellt einige integrierte Telefonieadapter zur Verfügung: www.adobe.com/go/learn_cnn_adaptors_de.

Sie können auch die Connect Pro Telephony-Java-API verwenden, um für beliebige Audiokonferenzanbieter einen geeigneten integrierten Telefonieadapter zu entwickeln. Weitere Informationen finden Sie unter Verwenden von Telefonie mit Adobe Acrobat Connect Pro.

Sie können Universal Voice für integrierte Telefonieadapter konfigurieren. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Universal Voice für integrierte Telefonieadapter“ auf Seite 46.

Folgende Tabelle zeigt die Funktionen beider Lösungen:

	Universal Voice-Audio-Anbieter	Integrierte Telefonieadapter
Audio an Teilnehmer übertragen, die nur über VoIP verfügen	Ja	Nein (falls nicht ein Adapter für Universal Voice konfiguriert wurde)

	Universal Voice-Audio-Anbieter	**Integrierte Telefonieadapter**
Erweiterte Anrufsteuerung. Beispielsweise: stumm, Warteschleife usw.	Nein	Ja
Aufzeichnen von Audio mit Connect Pro-Meeting	Ja	Ja
Erfordert Flash Media Gateway (Teil des Connect Pro-Installationsprogramms)	Ja	Nein (falls nicht ein Adapter für Universal Voice konfiguriert wurde)

Kapitel 2: Installieren von Connect Pro

Starten Sie zur Installation von Acrobat Connect Pro Server 7.5, Acrobat Connect Edge Server 7.5 und Flash Media Gateway das Installationsprogramm und befolgen Sie die Schritte des Assistenten der Anwendungsverwaltungskonsole.

Installieren von Connect Pro Server und Flash Media Gateway

Ausführen des Installationsprogramms

1 Melden Sie sich als Administrator an Ihrem Computer an.

2 Schließen Sie alle Anwendungen.

3 Legen Sie die Installations-DVD in das DVD-Laufwerk ein. Klicken Sie auf dem Startbildschirm auf die Schaltfläche zum Installieren von Adobe Acrobat Connect Pro Server 7.5.

Falls die Installation nicht automatisch gestartet wird, doppelklicken Sie auf die Datei „install.exe“ mit dem Pfad: „Connect\7.5\Disk1\InstData\VM\install.exe“.

4 Wählen Sie eine Sprache und klicken Sie auf „OK“.

5 Klicken Sie im Begrüßungsbildschirm auf „Weiter“, um den Vorgang fortzusetzen.

6 Wählen Sie eins der folgenden Produkte zur Installation aus und klicken Sie auf „Weiter“, um fortzufahren.

- Connect Pro-Server
- Flash Media Gateway

Hinweis: *Falls Sie keinen vorgelagerten SIP/VOIP-Anbieter nutzen, sollten Sie Flash Media Gateway nicht installieren. Weitere Informationen finden Sie unter* *„Audiokonferenzoptionen mit Connect Pro“ auf Seite 14.*

7 Lesen Sie den Text im Bildschirm mit der Lizenzvereinbarung durch, wählen Sie „Ich stimme der Vereinbarung zu“ und klicken Sie auf „Weiter“.

8 Wählen Sie den Installationsspeicherort für Connect Pro Server über eine der folgenden Optionen und klicken Sie auf „Weiter“.

- Klicken Sie auf „Weiter“, um den Standard-Installationsspeicherort für Connect Pro Server zu akzeptieren, oder klicken Sie auf „Auswählen“, um einen anderen Speicherort zu wählen.
- Falls Sie einen anderen Speicherort ausgewählt haben und dennoch den Standardspeicherort verwenden möchten, klicken Sie auf „Standardordner wiederherstellen“.
- Falls Acrobat Connect Pro bereits auf diesem Computer installiert ist, wird der Bildschirm „Vorhandene Connect Pro-Installation aktualisieren“ angezeigt. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie Ihre Datenbank und das Connect Pro-Stammverzeichnis mit einem Backup gesichert haben.

9 Wählen Sie den Installationsspeicherort für Flash Media Gateway über eine der folgenden Optionen und klicken Sie auf „Weiter“.

- Klicken Sie auf „Weiter“, um den Standard-Installationsspeicherort (C:\Programme\Adobe\Flash Media Gateway) zu akzeptieren, oder klicken Sie auf „Auswählen“, um einen anderen Speicherort zu wählen.

- Falls Sie einen anderen Speicherort ausgewählt haben und dennoch den Standardspeicherort verwenden möchten, klicken Sie auf „Standardordner wiederherstellen".
- Falls Flash Media Gateway bereits auf diesem Computer installiert ist, erscheint der Installationsbildschirm „Bestehendes Flash Media Gateway aktualisieren".

10 Geben Sie Ihre Seriennummer ein und klicken Sie auf „Weiter".

Hinweis: *Sie haben von Adobe eine E-Mail mit einem Link auf die Lizenzierungssite des Unternehmens erhalten. Aktivieren Sie diesen Link, um Ihre Seriennummer abzurufen.*

11 Falls der Bildschirm „Eingebettete Datenbank-Engine" angezeigt wird, führen Sie eine der folgenden Optionen durch:

- Falls die Datenbank auf einem anderen Computer installiert werden soll, wählen Sie die Option „Die eingebettete Datenbank-Engine nicht installieren".
- Um die eingebettete Datenbank zu installieren, wählen Sie die Option „Die eingebettete Datenbank-Engine an folgendem Speicherort installieren". Um den Standardspeicherort (C:\Programme\Microsoft SQL Server) für die Installation zu nutzen, klicken Sie auf „Weiter". Klicken Sie auf „Auswählen", um einen anderen Speicherort zu wählen.

Hinweis: *Falls das Installationsprogramm erkennt, dass Microsoft SQL Server bereits auf dem Computer installiert ist, installiert das Installationsprogramm die Datenbank nicht erneut. Falls es sich um eine Migration handelt und Sie die eingebettete Datenbank bereits nutzen, verwendet Connect Pro die bestehende Datenbank ebenfalls. In manchen Fällen erkennt jedoch das Installationsprogramm eine ältere Version von SQL Server, die nicht zusammen mit Connect Pro verwendet werden kann. Führen Sie die Schritte im Abschnitt „Deinstallieren von Acrobat Connect Pro Server" auf Seite 23 aus und starten Sie die Installation erneut.*

12 Geben Sie nach der Installation des Engines der eingebetteten Datenbank ein komplexes Kennwort ein und klicken Sie auf „Weiter".

13 Prüfen Sie abschließend die Preinstallationsübersicht. Klicken Sie auf „Zurück", um diese Einstellungen zu ändern. Klicken Sie auf „Installieren", um die Software zu installieren.

14 Führen Sie auf dem Bildschirm „Connect Pro wird initialisiert" die folgenden Schritte aus und klicken Sie auf „Weiter":

- Wählen Sie die Option „Connect Pro starten" (empfohlen).
- Wählen Sie „Connect Pro jetzt nicht starten...".

Falls Sie sich für das Starten von Connect Pro nach dem Neustart entscheiden, sollten Sie Connect Pro vor dem erstmaligen Ausführen konfigurieren. Um die Anwendungsverwaltungskonsole zum Konfigurieren von Connect Pro zu öffnen, wählen Sie „Start" > „Programme" > „Adobe Acrobat Connect Pro Server" > „Connect Pro Enterprise Server konfigurieren".

15 Nach dem Starten von Connect Pro wird in einer Meldung angezeigt, dass der Dienst gestartet wird.

Acrobat Connect Pro Server beinhaltet vier Windows-Dienste: Adobe Connect Enterprise Service, Flash Media Server (FMS), Flash Media Administration Server und Acrobat Connect Pro Presence Server. Flash Media Gateway wird in Form des Dienstes „Flash Media Gateway" ausgeführt. Weitere Informationen hierzu finden Sie unter „Starten und Beenden der Server" auf Seite 91.

16 Klicken Sie auf „Fertig stellen", um das Installationsprogramm zu verlassen.

Wenn Sie die Option „Connect Pro starten" auswählen, wird der Assistent der Anwendungsverwaltungskonsole in einem Browserfenster geöffnet und führt Sie durch die Konfiguration.

Konfigurieren von Acrobat Connect Pro mit dem Assistenten der Anwendungsverwaltungskonsole

Nach der Installation von Acrobat Connect Pro startet das Installationsprogramm den Assistenten der Anwendungsverwaltungskonsole. Der Assistent führt Sie durch die Konfiguration der Datenbank- und Servereinstellungen, den Upload der Lizenzdatei und das Erstellen eines Administratorkontos.

Hinweis: *Wenn auf Port 80 bereits eine andere Anwendung ausgeführt wird, kann die Anwendungsverwaltungskonsole nicht geöffnet werden. Beenden Sie die Anwendung an Port 80 und öffnen Sie die Anwendungsverwaltungskonsole.*

Sie können die Anwendungsverwaltungskonsole mit der Option „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server “ > „Connect Pro Enterprise Server konfigurieren“ starten oder die folgende URL verwenden: http://localhost:8510/console.

1. Lesen Sie den Begrüßungsbildschirm.

Er enthält einen Überblick über den Assistenten.

2. Geben Sie die Datenbankeinstellungen ein.

Legen Sie Werte für die unten aufgeführten Parameter fest. Klicken Sie auf „Weiter“, um eine Verbindung zur Datenbank herzustellen und Ihre Einstellungen zu überprüfen.

Datenbank-Host Der Hostname des Computers, auf dem die Datenbank installiert ist. Wenn Sie die eingebettete Datenbank installiert haben, lautet der Wert „localhost“.

Datenbankname Der Name der Datenbank. Der Standardwert lautet „breeze“.

Datenbank-Port Der Port der Datenbank, der für die Kommunikation mit Acrobat Connect Pro verwendet wird. Der Standardwert ist 1433. (Wenn Sie die eingebettete Datenbank-Engine verwenden, ändern Sie den Wert auf 1434.)

Datenbankbenutzer Der Name des Datenbankbenutzers. Wenn Sie die eingebettete Datenbank installiert haben, lautet der Standardwert „sa“.

Kennwort des Datenbankbenutzers Das Kennwort des Datenbankbenutzers. Falls Sie die eingebettete Datenbank installiert haben, richten Sie das Kennwort im Installationsprogramm ein.

3. Geben Sie die Servereinstellungen ein.

Benutzerkontoname Ein Name, der das Acrobat Connect Pro-Benutzerkonto definiert, zum Beispiel „Acrobat Connect Pro 7-Konto“.

Connect Pro-Host Ein vollständig qualifizierter Domänenname (FQDN), den Clients verwenden, um die Verbindung zu Acrobat Connect Pro herzustellen. Wenn die URL des Benutzerkontos beispielsweise „http://connect.beispiel.com“ lautet, ist der Wert für den Connect Pro-Host „connect.beispiel.com“.

HTTP-Port Der Port, den Acrobat Connect Pro für die Kommunikation via HTTP verwendet. Der Standardwert ist 80. Wenn Sie einen anderen Wert als 80 eingeben, müssen Clients die Portnummer zum Hostnamen in der URL hinzufügen, wenn sie auf das Acrobat Connect Pro-Konto zugreifen.

Hostzuordnungen „Name“ ist der Hostname des Computers, auf dem Acrobat Connect Pro gehostet wird. „Externer Name“ ist der FQDN, den Clients für die Verbindung mit Acrobat Connect Pro verwenden.

Hinweis: *Hängen Sie keine Portnummer an den FQDN im Feld „Externer Name“ an.*

SMTP-Host Der Hostname des Computers, der den SMTP-Mail-Server hostet.

SMTP-Benutzername Der Benutzername, der zur Authentifizierung am SMTP-Host verwendet wird. Wenn dieses Feld leer gelassen wird, versucht Connect Pro, E-Mails ohne Authentifizierung an den SMTP-Server zu senden.

SMTP-Kennwort Das Kennwort für den SMTP-Benutzernamen.

System-E-Mail Die E-Mail-Adresse, von der aus administrative Nachrichten gesendet werden.

Support-E-Mail Die E-Mail-Adresse des Supports für Acrobat Connect Pro-Benutzer.

BCC E-Mail Eine E–Mail-Adresse für verdeckte Kopien, an die alle Benutzerbenachrichtigungen ebenfalls gesendet werden. Mithilfe dieser Variablen können über Acrobat Connect Pro gesendete E-Mail-Meldungen für Verwaltungszwecke verfolgt werden, ohne eine interne E-Mail-Adresse preiszugeben.

Gemeinsamer Speicher Ein Datenträger und Verzeichnis auf einem externen Server für das Speichern von Materialien, zum Beispiel „\\Datenträger\Verzeichnis“. Wenn Sie Materialien auf mehreren Datenträgern speichern möchten, trennen Sie die Datenträgernamen durch Semikolons (;). Lesen Sie vor der Konfiguration dieser Funktion den Abschnitt „Konfigurieren von gemeinsamem Speicher“ auf Seite 48.

Größe des Content-Caches Eine ganze Zahl zwischen 1 und 100, die angibt, wieviel Prozent des verfügbaren Festplattenspeichers für die Speicherung von Materialien auf Acrobat Connect Pro verwendet werden. Der Cache kann größer werden als die angegebene Prozentzahl, deshalb sollte der Wert am besten zwischen 15 und 50 liegen. Wenn Sie das Feld nicht ausfüllen oder 0 eingeben, wird kein Cache verwendet und die Materialien werden auf Acrobat Connect Pro und ggf. vorhandenen externen Laufwerken gespiegelt. Lesen Sie vor der Konfiguration dieser Funktion bitte „Konfigurieren von gemeinsamem Speicher“ auf Seite 48.

4. Geben Sie die Flash Media Gateway-Einstellungen ein.

Geben Sie die Computernamen und die externen Namen für Flash Media Gateway-Server ein. Die Einstellungen werden nicht sofort wirksam. Nachdem Sie auf „OK“ klicken, um die Einstellungen zu bestätigen, startet Connect Pro möglicherweise alle Flash Media Gateway-Server neu. Die Einstellungen werden per Push an alle Flash Media Gateway-Server eines Clusters versendet.

Klicken Sie auf „Hinzufügen“, um Flash Media Gateway-Server hinzuzufügen. Übergeben Sie folgende Parameter:

Name Der Name des Computers, der als Host für Flash Media Gateway dient, beispielsweise „mustermann-pc“.

Externer Name Der FQDN des Computers, der als Host für Flash Media Gateway dient, beispielsweise „mustermann-pc.beispiel.com“.

Hinweis: *Hängen Sie keine Portnummer an den FQDN im Feld „Externer Name“ an.*

Der Status gibt an, ob Connect Pro Server sich mit dem Flash Media Gateway-Server verbinden kann, oder nicht. Der Flash Media Gateway-Server kann einige Sekunden benötigen, bis er einsatzbereit ist. Der Status „Aktiv“ bedeutet nicht, dass die SIP-Einstellungen bereits per Push an den Flash Media Gateway-Server übertragen wurden. Wenn sich Connect Pro Server nicht mit Flash Media Gateway verbinden kann, ist der Status „Inaktiv“.

Klicken Sie auf „Weiter“ und geben Sie die folgenden Parameter ein:

Benutzername Der Benutzername für das SIP-Profil, dass der Flash Media Gateway-Server verwendet, um SIP-Sessions zu erstellen, beispielsweise „sipUN1“.

Kennwort Das Kennwort für das SIP-Profil, dass der Flash Media Gateway-Server verwendet, um SIP-Sessions zu erstellen.

SIP-Adresse Die Adresse des SIP-Servers für das SIP-Profil, dass der Flash Media Gateway-Server verwendet, um SIP-Sessions zu erstellen, beispielsweise 10.12.13.14:12345.

Standardhost Den Standardhost für das SIP-Profil. Dieser Parameter ist die SIP-Serveradresse für den Fall, dass die Registrierung mit dem SIP-Server fehlschlägt. Für diesen Parameter wird gewöhnlich ein Wert gewählt, der identisch mit der SIP-Adresse ist.

Registrierung Wählen Sie, ob ein Flash Media Gateway-Server sich beim SIP-Server registrieren muss.

SIP-Port Der Port, auf dem der Flash Media Gateway-Server auf SIP-Anfragen wartet, beispielsweise 5060.

Untere Portgrenze Die niedrigste Portnummer, die für RTP-Audiodaten genutzt werden kann. Der Standardwert ist 5000.

Obere Portgrenze Die höchste Portnummer, die für RTP-Audiodaten genutzt werden kann. Der Standardwert ist 6000.

Ablauf der Registrierung Das Intervall in Sekunden, nach dessen Ablauf Flash Media Gateway die Registrierung mit dem SIP-Server erneuert. Der Standardwert beträgt 2400 Sekunden.

5. Laden Sie Ihre Lizenzdatei hoch

Acrobat Connect Pro wird erst aktiviert, wenn Sie eine Lizenzdatei von Adobe heruntergeladen und auf dem Computer, auf dem Acrobat Connect Pro gehostet wird, installiert haben. Klicken Sie auf den Link, um Ihre Lizenzdatei von Adobe herunterzuladen. Wechseln Sie dann zur heruntergeladenen Lizenzdatei, um sie in Ihr Acrobat Connect Pro-Installationsverzeichnis zu kopieren.

6. Erstellen Sie einen Administrator

Für jedes Acrobat Connect Pro-Benutzerkonto wird mindestens ein Administrator benötigt, um Aufgaben in der Webanwendung Connect Pro Central auszuführen. Benutzerkonten, für die ein Upgrade ausgeführt wurde, verfügen bereits über mindestens einen Administrator. Sie können hier bei Bedarf aber weitere hinzufügen.

7. Fahren Sie mit der Nutzung von Acrobat Connect Pro fort

Von hier aus können Sie sich bei Connect Pro Central anmelden (dies ist die Webanwendung, in der Sie Ihr Benutzerkonto verwalten, Meetings, Veranstaltungen usw. erstellen und Materialien auf dem Computer, der Acrobat Connect Pro hostet, verwalten), zur Anwendungsverwaltungskonsole zurückkehren (um Einstellungen zu überprüfen oder zu ändern) oder die Dokumentation aufrufen, um sich ausführlicher über Acrobat Connect Pro zu informieren.

Überprüfen der Installation

Überprüfen der Datenbankverbindung

Wenn Sie sich bei Connect Pro Central (einer Webanwendung innerhalb von Acrobat Connect Pro) anmelden können, funktioniert die Kommunikation zwischen der Datenbank und Acrobat Connect Pro korrekt.

1 Gehen Sie zur folgenden URL: http://*[hostname]* .

Hinweis: *In dieser URL ist [hostname] der Wert, den Sie in der Anwendungsverwaltungskonsole für Connect Pro festgelegt haben.*

2 Geben Sie den Benutzernamen und das Kennwort ein, das Sie in der Anwendungsverwaltungskonsole festgelegt haben.

Wenn Sie sich erfolgreich angemeldet haben, wird die Registerkarte „Home“ von Connect Pro Central angezeigt.

Überprüfen der Funktionsfähigkeit von E-Mail-Benachrichtigungen

Falls in der Anwendungsverwaltungskonsole kein Wert in das Feld „SMTP-Host“ eingegeben wurde, kann Acrobat Connect Pro keine E-Mail-Benachrichtigungen versenden. Falls ein SMTP-Host eingegeben wurde, prüfen Sie mit folgenden Schritten, ob Connect Pro E-Mail-Benachrichtigungen versenden kann.

1 Klicken Sie auf der Registerkarte „Home“ von Connect Pro Central auf die Registerkarte „Administration“.

2 Klicken Sie auf die Registerkarte „Benutzer und Gruppen“.

3 Klicken Sie auf „Neuer Benutzer“.

4 Geben Sie auf der Seite „Informationen zu neuem Benutzer“ die erforderlichen Daten ein. Es wird eine Liste mit Optionen angezeigt:

E-Mail Verwenden Sie die E-Mail-Adresse des neuen Benutzers. Vergewissern Sie sich, dass die Option „Kontoinformationen, Benutzername und Kennwort per E-Mail an neuen Benutzer senden“ aktiviert ist.

Neues Kennwort Erstellen Sie ein Kennwort mit 4 bis 16 Zeichen.

5 Klicken Sie auf „Weiter“, um fortzufahren.

6 Wählen Sie unter der Überschrift „Gruppenmitgliedschaft bearbeiten“ eine Gruppe aus, weisen Sie den Benutzer der Gruppe zu und klicken Sie auf „Fertig stellen“.

7 Planen Sie ausreichend Zeit ein, damit der Benutzer die E-Mail-Benachrichtigung erhalten und lesen kann.

Wenn der Benutzer die Benachrichtigung erhält, ist Acrobat Connect Pro einsatzbereit, und Sie können E-Mail-Nachrichten über Ihren E-Mail-Server senden.

8 Falls die E-Mail nicht beim Benutzer ankommt, führen Sie folgende Schritte aus:

a Vergewissern Sie sich, dass die E-Mail-Adresse gültig ist.

b Vergewissern Sie sich, dass die E-Mail nicht als Spam herausgefiltert wurde.

c Vergewissern Sie sich, dass Sie Acrobat Connect Pro mit einem gültigen SMTP-Host konfiguriert haben und dass der SMTP-Dienst außerhalb von Acrobat Connect Pro korrekt arbeitet.

d Wenden Sie sich an den Adobe-Support unter www.adobe.com/go/connect_licensed_programs_de.

Überprüfen der Funktionsfähigkeit von Adobe Presenter

Um die Funktionsfähigkeit von Adobe Presenter zu überprüfen, senden Sie eine Microsoft PowerPoint-Präsentation an Acrobat Connect Pro, damit sie in eine Flash-Präsentation kompiliert werden kann. Zeigen Sie die Präsentation dann an.

Bevor Sie eine PowerPoint-Präsentation an Acrobat Connect Pro senden können, müssen Sie Adobe Presenter auf einem Computer installieren, auf dem PowerPoint bereits installiert ist.

1 Starten Sie einen Browser und öffnen Sie Connect Pro Central (http://localhost:8510 oder den FQDN Ihres Connect Pro Servers).

2 Klicken Sie auf „Ressourcen“ > „Erste Schritte“.

3 Klicken Sie auf der Seite „Erste Schritte“ auf „Präsentationen veröffentlichen“ > „Adobe Presenter installieren“.

4 Ausführen des Installationsprogramms.

5 Falls Sie keine PowerPoint-Präsentation zur Hand haben, erstellen und speichern Sie eine ein- bis zweiseitige Präsentation.

6 Wählen Sie im PowerPoint-Menü „Adobe Presenter“ die Option „Veröffentlichen“ aus, um den Assistenten zum Veröffentlichen zu öffnen.

7 Wählen Sie „Connect Pro“ und geben Sie die Informationen für Ihren Server ein.

8 Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Kennwort an, und befolgen Sie die Schritte des Veröffentlichungsassistenten. Vergewissern Sie sich, dass Sie Mitglied der Autorengruppe sind („Administration“ > „Benutzer und Gruppen“ in Connect Pro Central).

Nach Abschluss der Schritte im Assistenten „Veröffentlichen“ lädt Adobe Presenter Ihre PowerPoint-Präsentation nach Connect Pro hoch, wo sie in eine Flash-Präsentation kompiliert wird.

9 Nach Abschluss der Kompilierung suchen Sie die Präsentation auf der Registerkarte „Material“ in Connect Pro Central.

10 Öffnen Sie die Präsentation, um sie anzuzeigen.

Überprüfen der Funktionsfähigkeit der Komponente „Schulung“

***Hinweis:** Adobe Acrobat Connect Pro Training ist eine optionale Funktion, die in Ihrer Lizenz aktiviert werden muss.*

❖ Klicken Sie in Connect Pro Central auf die Registerkarte „Schulung“.

Wenn Sie die Registerkarte „Schulung“ sehen und darauf klicken können, ist die Training-Schulungskomponente einsatzbereit. Vergewissern Sie sich, dass Sie Mitglied der Schulungsverwalter-Gruppe sind („Administration“ > „Benutzer und Gruppen“).

Überprüfen der Funktionsfähigkeit der Komponente „Meeting“

***Hinweis:** Adobe Acrobat Connect Pro Meeting ist eine optionale Funktion, die in Ihrer Lizenz aktiviert werden muss.*

Um zu überprüfen, ob Acrobat Connect Pro Meeting einsatzbereit ist, müssen Sie Mitglied der Meetingveranstalter-Gruppe oder der Administratoren-Gruppe sein.

1 Melden Sie sich als Benutzer, der Mitglied der Meetingveranstalter-Gruppe oder der Administratoren-Gruppe ist, bei Connect Pro an.

2 Klicken Sie auf die Registerkarte „Meetings“ und wählen Sie „Neues Meeting“.

3 Geben Sie auf der Seite „Meetinginformationen eingeben“ die erforderlichen Daten ein. Wählen Sie unter „Meetingzugriff“ die Option „Nur registrierte Benutzer und genehmigte Gäste dürfen den Raum betreten“. Klicken Sie auf „Fertig stellen“, um das Meeting zu erstellen.

4 Klicken Sie auf „Meetingraum betreten“.

5 Melden Sie sich als registrierter Benutzer beim Meeting an.

6 Wenn ein Fenster für das Acrobat Connect-Add-In angezeigt wird, befolgen Sie die Anweisungen für die Installation.

Wenn der Meetingraum geöffnet wird, ist Acrobat Connect Pro Meeting einsatzbereit.

Überprüfen der Funktionsfähigkeit von Events

***Hinweis:** Adobe Acrobat Connect Pro Events ist eine optionale Funktion, die in Ihrer Lizenz aktiviert werden muss.*

1 Melden Sie sich als Benutzer, der Mitglied der Eventveranstalter-Gruppe oder der Administratoren-Gruppe ist, bei Connect Pro Central an.

2 Klicken Sie in Connect Pro Central auf die Registerkarte „Veranstaltungen“.

Wenn Sie diese Registerkarte sehen und darauf klicken können, ist Connect Pro Events einsatzbereit.

Installieren von Acrobat Connect Pro Edge Server

Ausführen des Installationsprogramms

1 Schließen Sie alle anderen Anwendungen.

2 Legen Sie die Installations-DVD in das DVD-Laufwerk ein. Klicken Sie im Startbildschirm auf die Schaltfläche zum Installieren von Adobe Acrobat Connect Pro Edge Server

Falls das Installationsprogramm nicht automatisch gestartet wird, doppelklicken Sie im Stammverzeichnis der Installations-DVD auf „edgesetup.exe“.

3 Wählen Sie im Dialogfeld „Sprache auswählen“ eine Sprache aus. Klicken Sie auf „OK“, um den Vorgang fortzusetzen.

4 Klicken Sie im Setup-Bildschirm auf „Weiter“, um den Vorgang fortzusetzen.

5 Lesen Sie den Text im Bildschirm mit der Lizenzvereinbarung durch, wählen Sie „Ich stimme der Vereinbarung zu“ und klicken Sie auf „Weiter“.

6 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf „Weiter“, um den Standardordner für die Installation zu übernehmen (C:\\breeze). Wenn Sie einen anderen Speicherort wählen möchten, klicken Sie auf „Durchsuchen“, wählen Sie den gewünschten Ordner und klicken Sie dann auf „OK“.
- Falls Adobe Acrobat Connect Edge Server bereits auf diesem Computer installiert ist, wird der Bildschirm „Vorhandene Adobe Acrobat Connect Pro Edge Server-Installation aktualisieren“ angezeigt. Klicken Sie auf „Weiter“.

7 Führen Sie im Bildschirm „Startmenüordner auswählen“ einen der folgenden Schritte aus:

- Klicken Sie auf „Weiter“, um den Standardspeicherort der Startmenüverknüpfungen zu akzeptieren.
- Klicken Sie auf „Durchsuchen“, um einen unterschiedlichen Speicherort auszuwählen.

8 Überprüfen Sie im Dialogfeld „Bereit zur Installation“ den Installationsordner für Adobe Acrobat Connect Pro Edge Server und den Startmenü-Ordner. Klicken Sie ggf. auf „Zurück“, um diese Einstellungen zu ändern, oder klicken Sie auf „Installieren“.

9 Klicken Sie auf „Fertig stellen“, um die Adobe Acrobat Connect Pro Edge Server 7-Installation abzuschließen.

Verwandte Themen

„Bereitstellen von Acrobat Connect Pro Edge Server“ auf Seite 29

Deinstallieren der Server

Deinstallieren von Acrobat Connect Pro Server

Hinweis: *Beim Deinstallieren von Acrobat Connect Pro Server wird SQL Server nicht deinstalliert.*

1 Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server “ > „Connect Pro Server deinstallieren“.

2 Löschen Sie das Stammverzeichnis von Acrobat Connect Pro. Das Standardverzeichnis ist c:\breeze.

Wenn Sie Acrobat Connect Pro deinstallieren, werden die Dateien „custom.ini“ und „config.ini“ sowie die Materialdateien nicht gelöscht. Diese Dateien werden jedoch gelöscht, wenn Sie den Stammordner löschen.

Wichtig: *Der Stammordner enthält den Inhalteordner. Falls Sie die Inhalte weiter nutzen möchten, müssen sie an einen anderen Speicherort kopiert werden.*

3 Wählen Sie „Start“ > „Ausführen“. Geben Sie den Befehl **regedit** ein und klicken Sie anschließend auf „OK“, um den Registrierungseditor zu öffnen.

a Wechseln Sie zu „Arbeitsplatz“ -> HKEY_LOCAL_MACHINE -> SOFTWARE -> MICROSOFT -> WINDOWS -> AktuelleVersion -> Deinstallieren.

b Markieren und löschen Sie alle Schlüssel für Adobe Acrobat Connect Pro (die Titel können eine Versionszeichenkette enthalten).

4 (Optional) Wenn die eingebettete Datenbank-Engine installiert wurde, löschen Sie auch folgende Registrierungsschlüssel:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLSERVER

Deinstallieren von Acrobat Connect Pro Edge Server

1 Wählen Sie „Start“ > „Einstellungen“ > „Systemsteuerung“ > „Software“ > „Adobe Acrobat Connect Pro Edge Server “ > „Entfernen“.

2 Löschen Sie das Stammverzeichnis von Acrobat Connect Pro. Das Standardverzeichnis ist c:\breeze.

Deinstallieren von Flash Media Gateway

Beim Deinstallieren von Acrobat Connect Pro Server wird Flash Media Gateway ebenfalls deinstalliert. Flash Media Gateway kann auch durch das Ausführen des folgenden Programms deinstalliert werden: „Programme\Adobe\Flash Media Gateway\Uninstall_Flash Media Gateway\ Uninstall Flash Media Gateway.exe“.

Kapitel 3: Bereitstellen und Konfigurieren von Connect Pro

Nachdem Sie Adobe Acrobat Connect Pro Server, Flash Media Gateway oder Adobe Acrobat Connect Pro Edge Server installiert und die erste Phase der Konfiguration mithilfe der Anwendungsverwaltungskonsole abgeschlossen haben, konfigurieren Sie nach Bedarf folgende optionale Funktionen, und stellen Sie den Server bereit.

Bereitstellen von Acrobat Connect Pro Server

Bereitstellen von Acrobat Connect Pro Server

1 Legen Sie auf Ihrem DNS-Server einen FQDN (voll qualifizierenden Domainnamen) für Acrobat Connect Pro fest (z. B. verbinden.meinefirma.com). Ordnen Sie den Domainnamen der statischen IP-Adresse des Computers, auf dem Acrobat Connect Pro gehostet wird, zu.

2 Wenn Acrobat Connect Pro außerhalb Ihres Netzwerks verfügbar sein soll, konfigurieren Sie die folgenden Ports in einer Firewall:

80 Der Standardport für den Acrobat Connect Pro-Anwendungsserver. Der dritte Port für den Meetingserver (Flash Media Server).

1935 Der Standardport für den Meetingserver (Flash Media Server).

443 Der Standardport für SSL. Der zweite Port für den Meetingserver (Flash Media Server).

Hinweis: *Wenn der Acrobat Connect Pro-Datenverkehr über ein Gateway geleitet wird (mit einer anderen IP-Adresse), stellen Sie sicher, dass eine ggf. vorhandene Firewall für die Annahme von Anfragen durch die Gateway-IP-Adresse konfiguriert ist.*

Wenn Sie Hilfe beim Bereitstellen von Acrobat Connect Pro benötigen, wenden Sie sich an den Adobe-Support unter www.adobe.com/go/connect_licensed_programs_de.

Verwandte Themen

„Portanforderungen“ auf Seite 2

Bereitstellen eines Clusters aus Acrobat Connect Pro-Servern

Bevor Sie einen Cluster bereitstellen können, benötigen Sie Folgendes:

- Eine Lizenz, die die Anzahl der Knoten in Ihrem Cluster unterstützt. Weitere Informationen erhalten Sie bei Ihrem Adobe-Ansprechpartner.
- Jeder Computer im Cluster muss eine statistische IP-Adresse und einen DNS-Eintrag aufweisen.
- Einen E-Mail-Server.

- Eine SQL Server 2005-Standard-Installation auf einem dedizierten Computer mit einer statischen IP-Adresse. Wenn Sie Acrobat Connect Pro in einem Cluster installieren, können Sie die eingebettete Datenbank-Engine nicht nutzen. Jeder Server, auf dem Acrobat Connect Pro gehostet wird, erstellt eine Verbindung mit der Datenbank. Aufgrund von Lizenzbeschränkungen kann allerdings nicht mehr als ein Server eine Verbindung mit der eingebetteten Datenbankengine herstellen.
- Eine Hardware- oder Software-Lösung für die Lastverteilung. Eine Hardware für die Lastverteilung erfordert einen separaten Computer mit einer statischen IP-Adresse und einem DNS-Eintrag. Eine Software kann auf einem der Clusterknoten installiert werden.
- Mindestens ein Volume für den gemeinsamen Speicher. Diese Konfiguration ist nicht obligatorisch, wird jedoch empfohlen.

Bevor Sie Acrobat Connect Pro in einem Cluster bereitstellen, führen Sie zunächst eine erfolgreiche Installation auf einem einzelnen Computer aus. Konfigurieren Sie auch etwaige zusätzliche Funktionen (z. B. SSL, eine Verzeichnisdienstintegration, Single-Sign-On, gemeinsame Materialspeichernutzung) und überprüfen Sie, ob diese wie erwartet auf einem einzelnen Server funktionieren.

1 Installieren und konfigurieren Sie Acrobat Connect Pro auf einem dedizierten Server.

Verwenden Sie für jede Installation von Acrobat Connect Pro dieselbe Seriennummer und Lizenzdatei. Installieren Sie die eingebettete Datenbank-Engine nicht. Wenn der gemeinsame Speicher einen Benutzernamen und ein Kennwort erfordert, starten Sie Acrobat Connect Pro nicht über das Installationsprogramm.

2 Wenn der gemeinsame Speicher einen Benutzernamen und ein Kennwort erfordert, führen Sie folgende Schritte aus, um diese Informationen Adobe Connect Enterprise Service hinzuzufügen:

a Klicken Sie in der Systemsteuerung auf „Dienste“.

b Doppelklicken Sie auf „Adobe Connect Enterprise Service“.

c Klicken Sie auf die Registerkarte „Anmelden“.

d Aktivieren Sie das Optionsfeld „Dieses Konto“ und geben Sie den Benutzernamen für den gemeinsamen Speicher in das Textfeld ein. Die Syntax des Benutzernamens ist [subdomain\]Benutzername.

e Geben Sie das Kennwort für den gemeinsamen Speicher ein und bestätigen Sie die Eingabe.

f Klicken Sie auf „Anwenden“ und anschließend auf „OK“.

3 Führen Sie folgende Schritte aus, um Acrobat Connect Pro zu starten:

a Wählen Sie im Fenster „Dienste“ der Systemsteuerung die Option „Flash Media Server (FMS)“ und klicken Sie auf „Starten des Dienstes“.

b Wählen Sie im Fenster „Dienste“ der Systemsteuerung die Option „Adobe Connect Enterprise Service“ und klicken Sie auf „Starten des Dienstes“.

4 Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Server 7 konfigurieren“, um die Anwendungsverwaltungskonsole zu öffnen. Klicken Sie anschließend auf „Weiter“.

5 Geben Sie im Fenster „Datenbankeinstellungen“ die Informationen für die SQL Server-Datenbank ein und klicken Sie anschließend auf „Weiter“.

Wenn Acrobat Connect Pro erfolgreich eine Verbindung zur Datenbank hergestellt hat, werden die Datenbankeinstellungen sowie eine Bestätigung angezeigt. Klicken Sie auf „Weiter“.

6 Führen Sie im Fenster „Servereinstellungen“ die folgenden Schritte aus und klicken Sie auf „Weiter“:

a Geben Sie einen Kontonamen ein.

b Geben Sie im Feld „Connect Pro Host“ den Namen des Computers ein, auf dem der Load Balancer ausgeführt wird.

c Geben Sie eine HTTP-Portnummer ein. Je nach Load Balancer kann diese 80 oder 8080 lauten.

d Geben Sie den externen Namen des Clusterknotens ein.

e Geben Sie den Domänennamen des SMTP-Hosts und des Systems sowie Support-E-Mail-Adressen ein.

f Wenn Sie einen gemeinsamen Speicher verwenden, geben Sie den Pfad zum Volume ein (mehrere Volumes müssen durch Semikolons getrennt werden).

g Geben Sie den Prozentsatz des Acrobat Connect Pro-Servers an, der als lokaler Cache verwendet werden soll.

Hinweis: *Inhalte werden in den lokalen Cache und auf das Volume mit dem gemeinsamen Speicher geschrieben. Die Inhalte werden nach dem letzten Aufrufen 24 Stunden im lokalen Cache gespeichert. Wenn nach Ablauf dieser Frist der zugewiesene Cache-Prozentsatz überschritten wurde, werden die Inhalte gelöscht.*

7 Laden Sie die Lizenzdatei hoch und klicken Sie auf „Weiter“.

8 Erstellen Sie einen Administrator ein und klicken Sie auf „Fertig stellen“.

9 Wiederholen Sie die Schritte 1 bis 8 für jeden Server im Cluster.

10 Führen Sie zum Konfigurieren des Load Balancer folgende Schritte aus:

a Konfigurieren Sie den Load Balancer für Port 80.

b Fügen Sie der Konfigurationsdatei des Load Balancers die Namen aller Clusterknoten hinzu.

Hinweis: *Detaillierte Informationen zum Konfigurieren des Load Balancer finden Sie in der Dokumentation des Anbieters.*

11 Öffnen Sie einen Webbrowser und geben Sie den Domänennamen des Load Balancer ein, z. B. http://connect.beispiel.com.

Wenn Sie Hilfe beim Bereitstellen eines Clusters benötigen, wenden Sie sich an den Adobe-Support unter www.adobe.com/go/connect_licensed_programs_de.

Verwandte Themen

„Installieren von Connect Pro Server und Flash Media Gateway“ auf Seite 16

„Konfigurieren von gemeinsamem Speicher“ auf Seite 48

Überprüfen der Vorgänge in einem Cluster

Wenn ein Computer in einem Cluster heruntergefahren wird, leitet der Load Balancer alle HTTP-Anfragen an einen aktiven Computer im Cluster weiter.

Wenn ein Meeting beginnt, weist der Anwendungsserver dem Meetingraum basierend auf der Auslastung (Load) einen primären Host und einen Backup-Host zu. Wenn der primäre Host ausfällt, stellt der Client eine Verbindung zum Backup-Host her.

Sie sollten überprüfen, ob die auf einen Server hochgeladenen Materialien auf den anderen Computern im Cluster vervielfältigt werden.

In den folgenden Verfahren wird davon ausgegangen, dass der Cluster zwei Computer enthält: Computer1 und Computer2.

Überprüfen der Lastverteilung und Ausfallsicherungen für Meetings

1 Starten Sie Acrobat Connect Pro auf beiden Computern.

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server starten“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

2 Melden Sie sich über die folgende URL bei Connect Pro Central an:

http:// *[hostname]*

Verwenden Sie für *hostname* den Wert, den Sie in der Anwendungsverwaltungskonsole als Wert für „Connect Pro·Host“ eingegeben haben.

3 Wählen Sie die Registerkarte „Meetings“ und klicken Sie auf einen Meeting-Link, um einen Meetingraum zu betreten.

Erstellen Sie ggf. ein neues Meeting.

4 Beenden Sie Acrobat Connect Pro auf Computer2.

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server stoppen“.

Wenn die Meetingausfallsicherung funktioniert, sollte für das Meeting immer noch ein grünes Verbindungssymbol angezeigt werden.

5 Klicken Sie in Connect Pro Central auf eine beliebige Registerkarte oder auf einen Link.

Wenn der Load Balancer funktioniert, sollten Sie immer noch erfolgreich Anfragen an Connect Pro Central senden können und Antworten erhalten.

Wenn der Cluster mehr als zwei Computer enthält, probieren Sie dieses Starten-Stoppen-Verfahren für jeden Computer im Cluster aus.

Überprüfen der Materialvervielfältigung

1 Starten Sie Acrobat Connect Pro auf Computer1.

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server starten“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

2 Beenden Sie Acrobat Connect Pro auf Computer2.

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server stoppen“.

3 Melden Sie sich über die folgende URL bei Connect Pro Central an:

http:// *[hostname]*

Geben Sie für *hostname* den Wert ein, den Sie in der Anwendungsverwaltungskonsole als Wert für „Connect Pro·Host“ festgelegt haben.

4 Laden Sie ein JPEG-Bild oder anderes Material in Acrobat Connect Pro auf Computer1 hoch:

- Stellen Sie sicher, dass Sie Mitglied der Autorengruppe sind. (Als Administrator können Sie sich in Connect Pro Central selbst der Autorengruppe hinzufügen.)
- Klicken Sie auf die Registerkarte „Materialien“.
- Klicken Sie auf „Neue Materialien“ und folgen Sie den in Ihrem Browser angezeigten Schritten, um Material hinzuzufügen.

Wenn Sie Ihr Testmaterial hochgeladen haben, wird die Seite „Benutzermaterialien“ geöffnet. Hier wird eine Liste des Ihnen gehörenden Materials angezeigt.

5 Klicken Sie auf den Link des hochgeladenen Testmaterials.

Es wird eine Seite mit Materialinformationen eingeblendet, die eine URL enthält, über die Sie sich Ihr Testmaterial ansehen können.

6 Notieren Sie sich die URL. Sie benötigen sie für Schritt 10.

7 Klicken Sie auf die URL.

8 Starten Sie Computer2, warten Sie, bis Acrobat Connect Pro vollständig gestartet wurde, und beenden Sie dann Computer1.

Wenn Sie ein externes Speichergerät konfiguriert haben, brauchen Sie nicht zu warten, bis Computer2 beendet wurde; die Materialien werden vom externen Gerät kopiert.

9 Schließen Sie das Browserfenster, in dem das Testmaterial angezeigt wurde.

10 Öffnen Sie ein neues Browserfenster und geben Sie die URL für die Ansicht Ihres Testmaterials ein.

Wird das Testmaterial angezeigt, verlief die Vervielfältigung auf Computer2 erfolgreich. Wird ein leeres Fenster oder eine Fehlermeldung angezeigt, ist die Vervielfältigung fehlgeschlagen.

Bereitstellen von Acrobat Connect Pro Edge Server

Arbeitsablauf bei der Acrobat Connect Pro Edge Server-Installation

1. Definieren Sie Edge-Server-Zonen.

Sie können Edge-Server oder Cluster aus Edge-Servern an verschiedenen Standorten, so genannten *Zonen*einrichten, um den Zugriff auf Acrobat Connect Pro zu regeln und auszugleichen. So können Sie beispielsweise einen Edge-Server in München für Benutzer in Süddeutschland und einen Edge-Server in Hamburg für Benutzer in Norddeutschland einrichten.

2. Installieren von Acrobat Connect Pro Edge Server

Installieren Sie Acrobat Connect Pro Edge Server auf jedem Computer in jeder Zone. Wenn Sie beispielsweise einen Cluster aus Edge-Servern in einer Zone eingerichtet haben, installieren Sie Acrobat Connect Pro Edge Server auf jedem Computer im Cluster. Weitere Informationen hierzu finden Sie unter „Installieren von Acrobat Connect Pro Edge Server“ auf Seite 22

3. Ändern Sie den DNS-Server für jede Zone.

Ordnen Sie den FQDN des Acrobat Connect Pro-Ursprungsservers der statischen IP-Adresse von Acrobat Connect Pro Edge Server in jeder Zone zu. Weitere Informationen hierzu finden Sie unter „Bereitstellen von Acrobat Connect Pro Edge Server“ auf Seite 29.

4. Edge-Server konfigurieren.

Die Konfigurationsparameter müssen der Datei „custom.ini“ auf jedem Acrobat Connect Pro Edge Server hinzugefügt werden. Weitere Informationen hierzu finden Sie unter „Bereitstellen von Acrobat Connect Pro Edge Server“ auf Seite 29.

5. Konfigurieren Sie den Ursprungsserver.

Die Konfigurationsparameter müssen der Datei „custom.ini“ auf jedem Acrobat Connect Pro-server hinzugefügt werden. Außerdem müssen Sie den externen Namen des Edge-Servers in der Anwendungsverwaltungskonsole auf dem Ursprungsserver festlegen. Weitere Informationen hierzu finden Sie unter „Bereitstellen von Acrobat Connect Pro Edge Server“ auf Seite 29.

6. Richten Sie einen Load Balancer ein.

Wenn Sie mehrere Edge-Server in einer Zone einrichten, müssen Sie einen Lastausgleichmechanismus für die Edge-Server einrichten. Dieser Mechanismus muss so konfiguriert werden, dass Port 80 überwacht wird. Die Edge-Server überwachen Port 8080. Weitere Informationen finden Sie in der Dokumentation des Herstellers des Lastausgleichmechanismus.

Bereitstellen von Acrobat Connect Pro Edge Server

Bevor Sie Edge-Server bereitstellen, sollten Sie Acrobat Connect Pro und ggf. zusätzliche Funktionen (z. B. SSL, eine Verzeichnisserverintegration, Single Sign-On oder gemeinsamen Speicher) bereits erfolgreich implementiert haben.

1 Ordnen Sie auf Ihrem DNS-Server den FQDN des Ursprungsservers der statischen IP-Adresse des Edge-Servers zu. Wenn Sie Edge-Server in mehreren Zonen installieren, wiederholen Sie diesen Schritt für jede Zone.

***Hinweis:** Alternativ dazu können Sie eine Hostdatei verwenden. In diesem Fall benötigt jeder Client eine Hostdatei, die die statische IP-Adresse des Edge-Servers auf den FQDN des Ursprungsservers verweist.*

2 Öffnen Sie in Acrobat Connect Pro Edge Server die Datei *[Stamminstallationsverzeichnis]*\edgeserver\win32\conf\HttpCache.xml und ersetzen Sie den Computernamen im Tag HostName durch den FQDN des Edge-Server-Computers, z. B. edge1.beispiel.com.

```
<!-- The real name of this host. -->
<HostName>edge1.yourcompany.com</HostName>
```

3 Erstellen Sie auf Acrobat Connect Pro Edge Server die neue Datei *[root_install_dir]*\edgeserver\custom.ini und geben Sie die folgenden Parameter und Werte ein:

FCS_EDGE_HOST Die FQDN des Edge-Servers, beispielsweise, `FCS_EDGE_HOST=edge1.yourcompany.com`.

FCS_EDGE_REGISTER_HOST Der FQDN des Acrobat Connect Pro-Ursprungsservers, z. B. `FCS_EDGE_REGISTER_HOST=connect.yourcompany.com`.

FCS_EDGE_CLUSTER_ID Der Name des Clusters. Jeder Edge-Server-Cluster benötigt eine eindeutige ID. Alle Computer in einem Cluster müssen dieselbe ID haben. Das empfohlene Format ist *`companyname-clustername`*, z. B. `FCS_EDGE_CLUSTER_ID=yourcompany-us`.

***Hinweis:** Auch wenn Sie nur einen Acrobat Connect Pro Edge Server bereitstellen, müssen Sie diesen Parameter konfigurieren.*

FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT Die IP-Adresse oder der Domänenname und die Portnummer des Computers, auf dem Acrobat Connect Pro installiert ist, z. B. `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80`. An dieser Stelle ist Acrobat Connect Pro Edge Server mit dem Acrobat Connect Pro-Ursprungsserver verbunden.

FCS_EDGE_PASSWORD (Optional) Ein Kennwort für den Edge-Server. Wenn Sie einen Wert für diesen Parameter festlegen, müssen Sie denselben Wert für jeden Edge-Server und Ursprungsserver verwenden.

FCS_EDGE_EXPIRY_TIME (Optional) Die Anzahl der Millisekunden, innerhalb derer der Edge-Server sich beim Ursprungsserver registrieren muss, bevor eine Zeitsperre für den Cluster eintritt und das System einen anderen Edge-Server verwendet. Mit Standardwert starten, `FCS_EDGE_EXPIRY_TIME=60000`.

FCS_EDGE_REG_INTERVAL (Optional) Das Intervall, in Millisekunden, nach dem der Edge-Server die Registrierung beim eigentlichen Server versucht. Dieser Parameter legt fest, wie oft sich der Edge Server für den Ursprungsserver verfügbar macht. Mit Standardwert starten, `FCS_EDGE_REG_INTERVAL=30000`.

DEFAULT_FCS_HOSTPORT (Optional) Um die Edge Server-Ports zu konfigurieren, geben Sie die folgende Zeile ein: `DEFAULT_FCS_HOSTPORT=:1935,80,-443`

Mit dem Minuszeichen (-) vor 443 wird Port 443 als sicherer Port ausgewiesen, der nur RTMPS-Verbindungen akzeptiert. Wenn Sie eine RTMPS-Verbindung über Port 1935 oder 80 herzustellen versuchen, schlägt die Verbindung fehl. Aber auch eine unsichere RTMP-Verbindung an Port 443 wird nicht funktionieren.

Hinweis: *Wenn der Edge-Server eine externe Hardwarebeschleunigung einsetzt, muss der Port 443 nicht als sicherer Port konfiguriert werden.*

Die folgenden Werte sind Probewerte für die config.ini-Datei:

```
FCS_EDGE_HOST=edge.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=yourcompany-us
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

4 Starten Sie den Edge Server neu.

5 Öffnen Sie auf dem Acrobat Connect Pro-Ursprungsserver die Datei *[Stamm-Installationsverzeichnis]* \custom.ini in einem Texteditor und ordnen Sie den Wert des `FCS_EDGE_CLUSTER_ID`-Parameters einer Zonen-ID zu; die Syntax ist `Edge.`*`FCS_EDGE_CLUSTER_ID = Zonen-ID`*. Auch wenn Sie nur einen Edge-Server bereitstellen, müssen Sie die Cluster-ID einer Zonen-ID zuordnen.

Jeder Edge-Server-Cluster benötigt eine Zonen-ID. Die Zonen-ID kann eine beliebige positive ganze Zahl sein, die größer als Null ist. Sie könnten zum Beispiel drei Cluster haben, die den Zonen 1 bis 3 zugeordnet sind:

```
edge.yourcompany-us=1
edge.yourcompany-apac=2
edge.yourcompany-emea=3
```

Nachstehend finden Sie ein Beispiel für die Datei custom.ini des Ursprungsservers:

```
DB_HOST=localhost
DB_PORT=1433
DB_NAME=breeze
DB_USER=sa
DB_PASSWORD=#V1#4cUsRJ6oeFwZLnQPpS4f0w==
# DEBUG LOGGING SETTINGS
HTTP_TRACE=yes
DB_LOG_ALL_QUERIES=yes
# EDGE SERVER SETTINGS
edge.yourcompany-us=1
```

Hinweis: *Wenn Sie in der Datei config.ini auf dem Edge-Server einen Parameter* `FCS_EDGE_PASSWORD` *festlegen, müssen Sie dasselbe Kennwort in der Datei custom.ini auf dem Ursprungsserver festlegen.*

6 Starten Sie den Ursprungsserver neu.

7 Öffnen Sie auf dem Ursprungsserver die Anwendungsverwaltungskonsole („Start“ > „Programme“ > „ Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Server 7 konfigurieren“). Wählen Sie die Registerkarte „Anwendungseinstellungen“ und dann „Servereinstellungen“ und geben Sie im Bereich „Hostzuordnungen“ den externen Namen für den Edge-Server ein. Der externe Name sollte dem Wert entsprechen, der für den Parameter `FCS_EDGE_HOST` auf dem Edge-Server festgelegt ist.

8 Konfigurieren Sie auf dem Ursprungsserver die Windows-Firewall so, dass die Edge-Server auf Port 8506 zugreifen können.

9 Wiederholen Sie die Schritte 2 bis 4 für jeden Edge-Server in jeder Zone.

10 Wiederholen Sie die Schritte 5 bis 7 für jeden Ursprungsserver in jeder Zone.

Wenn Sie Hilfe beim Bereitstellen von Edge-Servern benötigen, wenden Sie sich an den Adobe-Support unter www.adobe.com/go/connect_licensed_programs_de.

Verwandte Themen

„Auswahl der Bereitstellung von Acrobat Connect Pro Edge Server“ auf Seite 12

Integration mit einem Verzeichnisdienst

Überblick über die Verzeichnisdienstintegration

Sie können Acrobat Connect Pro mit einem Verzeichnisdienst integrieren, um Benutzer anhand des LDAP-Verzeichnisses zu authentisieren und um das manuelle Hinzufügen einzelner Benutzer und Gruppen zu verhindern. Benutzerkonten werden in Acrobat Connect Pro automatisch über manuelle oder geplante Synchronisationen mit dem Verzeichnis Ihrer Organisation erstellt.

Für die Integration mit Acrobat Connect Pro muss Ihr Verzeichnisserver Lightweight Directory Access Protocol (LDAP) oder sicheres Lightweight Directory Access Protocol (LDAPS) verwenden. LDAP ist ein Client-Server-Netzwerkprotokoll für das Nachschlagen von Benutzerkontaktinformationen in einem LDAP-kompatiblen Verzeichnisserver.

Acrobat Connect Pro erstellt als LDAP-Client eine Verbindung zu einem LDAP-Verzeichnis. Acrobat Connect Pro importiert Benutzer und Gruppen und synchronisiert Informationen zu diesen Benutzern und Gruppen mit dem LDAP-Verzeichnis. Sie können Acrobat Connect Pro auch konfigurieren, um Benutzer anhand des LDAP-Verzeichnisses zu authentifizieren.

Jeder LDAP-kompatible Verzeichnisdienst kann mit Acrobat Connect Pro integriert werden. Eine Liste der unterstützten LDAP-Verzeichnisse finden Sie unter www.adobe.com/go/connect_sysreqs_de.

Informationen zur LDAP-Verzeichnisstruktur

LDAP-Verzeichnisse organisieren Informationen gemäß dem Standard X.500.

Ein Benutzer oder eine Gruppe in einem LDAP-Verzeichnis wird als *Eintrag* bezeichnet. Ein Eintrag besteht aus mehreren Attributen. Ein Attribut besteht aus einem Typ und einem oder mehreren Werten. Typen verwenden mnemonische Zeichenfolgen, wie `ou` für organizational unit (Organisationseinheit) oder `cn` für common name (üblicher Name). Attributwerte bestehen aus Informationen wie Telefonnummer, E-Mail-Adresse und Foto. Wenden Sie sich an Ihren LDAP-Administrator, um sich über die Struktur des LDAP-Verzeichnisses Ihrer Organisation zu informieren.

Jeder Eintrag verfügt über einen *distinguished name* (DN, eindeutiger Name), der den Pfad zu einem Eintrag über eine Baumstruktur vom Eintrag bis zum Stamm beschreibt. Der DN für einen Eintrag im LDAP-Verzeichnis ist eine Verkettung aus dem Namen des Eintrags (RDN oder *relative distinguished name*, relativer eindeutiger Name genannt) und den Namen der übergeordneten Einträge in der Baumstruktur.

Eine Baumstruktur kann geografische Bezeichnungen oder Abteilungen innerhalb eines Unternehmens darstellen. Wenn beispielsweise Alicia Solis ein Benutzer aus der QA-Abteilung von Acme, Inc. in Frankreich (c = country/Land) ist, könnte der DN für diesen Benutzer folgendermaßen lauten:

cn=Alicia Solis, ou=QA, c=Frankreich, dc=Acme, dc=com

Verzeichniszweige importieren

Beim Importieren von Benutzern und Gruppen aus einem LDAP-Verzeichnis in Acrobat Connect Pro geben Sie einen Pfad zu einem Abschnitt der LDAP-Baumstruktur an, indem Sie den DN des Abschnitts verwenden. Damit wird der Umfang der Suche festgelegt. Sie können zum Beispiel nur die Benutzer einer bestimmten Gruppe innerhalb Ihrer Organisation importieren. Dazu muss Ihnen bekannt sein, wo sich die Einträge für diese Gruppe in der Verzeichnisbaumstruktur befinden.

Eine übliche Methode ist die Verwendung der Internet-Domäne der Organisation als Stamm der Baumstruktur. Beispielsweise könnte Acme, Inc. `dc=com` verwenden, um das Stammelement im Baum zu spezifizieren. Ein DN, der das Vertriebsbüro von Acme, Inc. in Singapur spezifiziert, könnte `ou=Singapur`, `ou=Marketing`, `ou=Mitarbeiter`, `dc=Acme` oder `dc=com` lauten. (In diesem Beispiel steht `ou` als Abkürzung für organizational unit (Organisationseinheit) und `dc` für domain component (Domänenkomponente).)

Hinweis: *Nicht alle LDAP-Verzeichnisse verfügen über einen einzelnen Stamm. In diesem Fall können Sie separate Verzweigungen importieren.*

Benutzer und Benutzergruppen hinzufügen

Es gibt zwei Möglichkeiten, Benutzer- und Gruppeneinträge in einem LDAP-Verzeichnis anzuordnen: unter demselben Knoten einer Verzweigung oder unter verschiedenen Verzweigungen.

Wenn sich Benutzer und Gruppen unter demselben Knoten in einer LDAP-Verzweigung befinden, können Benutzer- und Gruppeneinstellungen für den Import von Einträgen denselben Verzweigungs-DN enthalten. Das bedeutet, dass Sie beim Importieren von Benutzern einen Filter einsetzen müssen, um nur Benutzer auszuwählen. Beim Importieren von Gruppen müssen Sie einen Filter verwenden, um nur Gruppen auszuwählen.

Wenn sich Benutzer und Gruppen unter verschiedenen Verzweigungen in der Baumstruktur befinden, verwenden Sie einen Verzweigungs-DN, der die Benutzerverzweigung auswählt, wenn Sie Benutzer importieren, bzw. die Gruppenverzweigung, wenn Sie Gruppen importieren.

Sie können auch untergeordnete Verzweigungen importieren, um Benutzer aus allen Verzweigungen unterhalb einer bestimmten Ebene zu importieren. Wenn Sie zum Beispiel alle Mitarbeiter der Vertriebsabteilung importieren möchten, können Sie den folgenden Verzweigungs-DN verwenden:

```
ou=Sales, dc=Acme, dc=com
```

Die Vertriebsmitarbeiter können jedoch auch in untergeordneten Verzweigungen organisiert sein. Stellen Sie in diesem Fall den Parameter für die Suche in untergeordneter Struktur auf „`true" (wahr)`, um sicherzustellen, dass Benutzer aus den dieser Ebene untergeordneten Strukturen des Baums importiert werden.

Ausgewählte Einträge filtern

Ein Filter legt Kriterien fest, die erfüllt sein müssen, damit ein Eintrag ausgewählt wird. Damit wird die Auswahl von Einträgen innerhalb eines Strukturbereichs eingeschränkt. Wenn der Filter beispielsweise `(objectClass=organizationalPerson)` spezifiziert, werden nur Einträge, die über das Attribut `organizationalPerson (Person aus dem Unternehmen)` verfügen, für einen Import ausgewählt.

Hinweis: *Das Attribut* `objectClass` *muss in jedem Eintrag eines LDAP-Verzeichnisses vorhanden sein.*

Interne und externe Benutzer und Gruppen

Benutzer und Gruppen, die Sie direkt in Acrobat Connect Pro erstellen, anstatt sie aus einem LDAP-Verzeichnis zu importieren, werden *interne* Benutzer und Gruppen genannt. Benutzer und Gruppen, die Sie aus einem LDAP-Verzeichnis in die Acrobat Connect Pro-Datenbank importieren, werden als *externe* Benutzer bezeichnet.

Damit die importierten Gruppen mit dem externen LDAP-Verzeichnis übereinstimmen, können Sie keine internen Benutzer und Gruppen zu externen Gruppen hinzufügen. Sie können internen Gruppen jedoch externe Benutzer und Gruppen hinzufügen.

Wenn der Wert des Anmeldenamens oder Namens eines importierten Benutzers oder einer importierten Gruppe mit dem eines vorhandenen internen Benutzers oder einer vorhandenen internen Gruppe übereinstimmt, wird beim Synchronisieren der Verzeichnisse der importierte Benutzer bzw. die importierte Gruppe von extern in intern geändert, und im Synchronisationsprotokoll wird eine entsprechende Warnung verzeichnet.

Integrieren von Acrobat Connect Pro mit einem LDAP-Verzeichnis

Sie integrieren Verzeichnisdienste in der Anwendungsverwaltungskonsole auf der Registerkarte „Einstellungen für Verzeichnisdienst“. Benutzen Sie ein Administratorkonto.

Sie können einen Verzeichnisserver zur Benutzerauthentifizierung und LDAP-Synchronisation konfigurieren. Die Konfiguration kann auf eine oder mehrere Verzweigungen des Verzeichnisdienstes ausgelegt sein.

1. Öffnen Sie die Anwendungsverwaltungskonsole.

Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Server 7 konfigurieren“.

2. Geben Sie die LDAP-Server-Verbindungseinstellungen ein.

Wählen Sie die Registerkarte „Einstellungen für Verzeichnisdienst“ aus. Geben Sie im Bildschirm „LDAP-Einstellungen“ > „Verbindungseinstellungen“ die erforderlichen Informationen ein und klicken Sie auf „Speichern“.

Wenn Sie auf „Speichern“ klicken, testet Acrobat Connect Pro die LDAP-Verbindung. Wenn der Test fehlschlägt, wird die folgende Nachricht angezeigt: „Die Einstellungen wurden erfolgreich gespeichert, die LDAP-Konnektivität konnte jedoch nicht überprüft werden.“ Bitte überprüfen Sie Ihre LDAP-URL und den Port.

Feld	**Standardwert**	**Beschreibung**
URL für LDAP-Server	Kein Standardwert.	Normalerweise in der Form „`ldap://`***`[servername:portnumber]`***“. Wenn Ihre Organisation einen sicheren LDAP-Server verwendet, geben Sie „`ldaps://"` ein. Wenn Sie keinen Port angeben, nutzt Acrobat Connect Pro den Standard-LDAP-Port (389) oder den LDAPS-Port (636) LDAPS erfordert SSL-Zertifikate. Wenn Sie Acrobat Connect Pro für die Nutzung in einem Microsoft Active Directory-Wald konfigurieren, in dem der globale Katalog aktiviert ist, nutzen Sie den globalen Katalog (Standardport: 3268).
Authentisierungs-methode für LDAP-Verbindung	Kein Standardwert	Der Mechanismus zur Authentifizierung der Anmeldedaten (LDAP-Benutzername, LDAP-Kennwort) des LDAP-Dienstkontos für Acrobat Connect Pro (Administratorrechte). **Einfach** (Standardauthentifizierung – empfohlen). **Anonym** (kein Kennwort – Ihr LDAP-Server muss zur Zulassung anonymer Anmeldungen konfiguriert sein). **Digest MD5** (konfigurieren Sie Ihren LDAP so, dass Digest-Authentifizierung zulässig ist).
Benutzername für LDAP-Verbindung	Kein Standardwert	Administrative Anmeldung am LDAP-Server.
LDAP-Verbindungskennwort	Kein Standardwert	Administratives Kennwort des LDAP-Servers.
Zeitüberschreitung bei LDAP-Abfrage	Kein Standardwert	Zeit in Sekunden, die vor dem Abbrechen der Abfrage verstreichen kann. Wenn Sie dieses Feld leer lassen, gibt es keine Zeitsperre. Setzen Sie diesen Wert auf 120.
Größenbeschränkung der LDAP-Abfrageseite	Kein Standardwert	Die Größe der Ergebnisseiten, die vom LDAP-Server zurückgegeben werden. Wenn dieses Feld leer gelassen wird oder den Wert „0“ hat, wird keine Abfrageseitengröße verwendet. Verwenden Sie dieses Feld für LDAP-Server, bei denen eine maximale Ergebnisgröße konfiguriert ist. Stellen Sie die Seitengröße auf einen Wert, der kleiner ist als die maximale Ergebnisgröße, damit alle Ergebnisse vom Server auf mehreren Seiten abgerufen werden. Wenn Sie beispielsweise versuchen, ein großes LDAP-Verzeichnis zu integrieren, das nur 1000 Benutzer anzeigen kann, jedoch 2000 Benutzer zu importieren sind, schlägt die Integration fehl. Setzen Sie die Abfrageseitengröße jedoch auf 100, werden die Ergebnisse auf 20 Seiten zurückgegeben und alle Benutzer werden importiert.

Nachstehend finden Sie ein Beispiel der LDAP-Syntax für Verbindungseinstellungen:

```
URL:ldap://ldapserver.mycompany.com
UserName:MYCOMPANY\jdoe
Password:password123
Query timeout:120
Authentication mechanism:Simple
Query page size:100
```

3. Ordnen Sie Acrobat Connect Pro- und LDAP-Verzeichnis-Benutzerprofilen zu

Wählen Sie die Registerkarte „Benutzerprofilzuordnung“, geben Sie Daten ein und klicken Sie auf „Speichern“.

Feld	**Standardwert**	**Beschreibung**
Anmelden	Kein Standardwert	Das Anmeldeattribut des Verzeichnisdienstes.

Feld	**Standardwert**	**Beschreibung**
Vorname	Kein Standardwert	Das Vornamenattribut des Verzeichnisdienstes.
Nachname	Kein Standardwert	Das Nachnamenattribut des Verzeichnisdienstes.
E-Mail	Kein Standardwert	Das E-Mail-Attribut des Verzeichnisdienstes.

Wenn Sie benutzerdefinierte Felder festgelegt haben, werden sie dem Bildschirm „Benutzerprofilzuordnung“ hinzugefügt. In diesem Beispiel wird ein Acrobat Connect Pro-Benutzerprofil einem Active Directory LDAP-Benutzerprofil zugeordnet; „Netzwerkanmeldung“ ist ein benutzerdefiniertes Feld.

```
Login:mail
FirstName:givenName
LastName:sn
Email:userPrincipalName
NetworkLogin:mail
```

4. (Optional) Fügen Sie eine Benutzerverzweigung hinzu.

Klicken Sie auf „Hinzufügen“, um Benutzerinformationen aus einer bestimmten Verzweigung Ihres Unternehmens hinzuzufügen. Geben Sie Werte in die Felder „Verzweigung“ und „Filter“ ein und klicken Sie auf „Speichern“.

Wenn Sie Benutzer aus untergeordneten Verzweigungen importieren möchten, wählen Sie im Menü zur Suche in untergeordneter Struktur „True“ (Wahr) aus. Anderenfalls wählen Sie „False“ (Falsch) aus.

Weitere Informationen finden Sie unter „Informationen zur LDAP-Verzeichnisstruktur“ auf Seite 32.

Feld	**Standardwert**	**LDAP-Attribut / Hinweise**
Verzweigungs-DN	Kein Standardwert	DN (Distinguished Name) des Stammknotens der Verzweigung. Ein Link zur gewählten Verzweigung wird angezeigt.
Filtern	Kein Standardwert	Die Zeichenfolge für den Abfragefilter.
Suche in untergeordneter Struktur	Richtig	True (wahr) oder False (falsch). Der Wert „True“ ermöglicht die rekursive Suche durch alle Unterverzweigungen dieser Verzweigung.

5. Zuordnen von Acrobat Connect Pro- und LDAP-Verzeichnis-Gruppenprofilen

Wählen Sie die Registerkarte „Gruppenprofilzuordnung“, geben Sie Werte ein und klicken Sie auf „Speichern“.

Hinweis: *Acrobat Connect Pro-Gruppenprofile unterstützen keine benutzerdefinierten Felder.*

Feld	**Standardwert**	**LDAP-Attribut / Hinweise**
Gruppenname	Kein Standardwert	Das Gruppennamenattribut des Verzeichnisdienstes.
Gruppenmitglied	Kein Standardwert	Das Gruppenmitgliedattribut des Verzeichnisdienstes.

Nachstehend sehen Sie eine Zuordnung von LDAP-Gruppeneintragsattributen zu einem Acrobat Connect Pro-Gruppenprofil:

```
Name:cn
Membership:member
```

6. (Optional) Fügen Sie eine Gruppenverzweigung hinzu.

Klicken Sie auf „Hinzufügen“, um Benutzerinformationen aus einer Verzweigung Ihrer Organisation hinzuzufügen. Geben Sie Werte in die Felder „Verzweigung“ und „Filter“ ein und klicken Sie auf „Speichern“.

Wenn Sie Gruppen aus untergeordneten Verzweigungen importieren möchten, wählen Sie im Menü zur Suche in untergeordneter Struktur „True“ (Wahr) aus. Anderenfalls wählen Sie „False“ (Falsch) aus.

Weitere Informationen finden Sie unter „Informationen zur LDAP-Verzeichnisstruktur“ auf Seite 32.

Feld	**Standardwert**	**LDAP-Attribut / Hinweise**
Verzweigungs-DN	Kein Standardwert	DN (Distinguished Name) des Stammknotens der Verzweigung. Jede Verzweigung eines Unternehmens verfügt über eigene LPAD-DN-Attribute. Ein Link zur gewählten Verzweigung wird angezeigt.
Filtern	Kein Standardwert	Die Zeichenfolge für den Abfragefilter.
Suche in untergeordneter Struktur	True	Ein boolescher Wert „`true" (wahr)` oder „`false" (falsch)`. Der Wert „`true"` ermöglicht die rekursive Suche durch alle Unterverzweigungen dieser Verzweigung.

Das folgende Beispiel zeigt das Hinzufügen einer Verzweigung zu einem Unternehmen und die Festlegung ihrer Gruppen in LDAP-Syntax:

```
DN:cn=USERS,DC=myteam,DC=mycompany,DC=com
Filter:(objectClass=group)
Subtree search:True
```

7. Geben Sie die Authentifizierungseinstellungen ein.

Wählen Sie die Registerkarte „Authentifizierungseinstellungen“ aus. Wenn Sie Acrobat Connect Pro-Benutzer anhand des Verzeichnisdienstes Ihrer Organisation authentifizieren möchten, wählen Sie „LDAP-Authentifizierung aktivieren“. Wenn Sie diese Option nicht auswählen, verwendet Acrobat Connect Pro native Authentifizierungen (in der Acrobat Connect Pro-Datenbank gespeicherte Benutzeranmeldedaten).

Wenn Sie die Option „Fallback von Connect Pro bei nicht erfolgreicher Authentifizierung über LDAP-Verzeichnis ermöglichen“ aktivieren, nutzt Acrobat Connect Pro die native Authentifizierung.

Hinweis: *Diese Option kann hilfreich sein, wenn es in Ihrem Netzwerk zu einem vorübergehenden Ausfall der LDAP-Konnektivität kommt. LDAP-Anmeldedaten können sich allerdings von denen in der Acrobat Connect Pro-Datenbank unterscheiden.*

Aktivieren Sie „Bei erfolgreicher Authentifizierung über LDAP-Verzeichnis Connect Pro-Benutzerkonto erstellen“, um Vorsorgen für Erstbenutzer auf dem Acrobat Connect Pro-Server zu treffen, wenn die LDAP-Authentifizierung erfolgreich ist. Lassen Sie diese Option aktiviert, wenn ein beliebiger Benutzer in Ihrem Verzeichnisdienst die Erlaubnis hat, Acrobat Connect Pro zu nutzen, und wählen Sie den Benutzerkontentyp „Intern“. Weitere Informationen finden Sie unter „Interne und externe Benutzer und Gruppen“ auf Seite 34.

Aktivieren Sie „Gruppeneinschreibung nur bei Erstanmeldung zulassen“, um in Acrobat Connect Pro einen Anmeldenamen zu erstellen und Benutzer in bestimmte Gruppen einzuteilen, wenn sie sich zum ersten Mal bei Acrobat Connect Pro anmelden. Geben Sie die Gruppennamen im entsprechenden Textfeld ein.

8. Planen Sie die Synchronisation.

Wählen Sie die Registerkarte „Synchronisationseinstellungen“ aus. Wählen Sie im Bildschirm „Planeinstellungen“ das Kontrollkästchen „Geplante Synchronisation aktivieren“, wenn Sie täglich, wöchentlich oder monatlich zu einer bestimmten Zeit Synchronisationen ausführen möchten. Weitere Informationen finden Sie unter „Empfohlene Verfahren für die Synchronisation“ auf Seite 38.

Sie können im Bildschirm „Synchronisationsaktionen“ auch eine manuelle Synchronisation ausführen.

9. Legen Sie Kennwort- und Löschungsrichtlinien fest.

Klicken Sie auf die Registerkarte „Richtlinieneinstellungen“, wählen Sie eine Richtlinie zur Kennworteinrichtung sowie eine Richtlinie zum Löschen und klicken Sie auf „Speichern“. Weitere Informationen zu Kennwortrichtlinien finden Sie unter „Verwalten von Kennwörtern“ auf Seite 38.

Hinweis: *Wenn Sie während einer Synchronisation die Option „Benutzer und Gruppen, die...“ auswählen, werden alle externen Benutzer, die vom LDAP-Server gelöscht wurden, auch vom Acrobat Connect Pro-Server gelöscht.*

10. Zeigen Sie eine Vorschau der Synchronisation an.

Wählen Sie die Registerkarte „Synchronisationsaktionen“ Klicken Sie im Bereich „Vorschau der Verzeichnissynchronisation“ auf „Vorschau“. Weitere Informationen finden Sie unter „Empfohlene Verfahren für die Synchronisation“ auf Seite 38.

Verwalten von Kennwörtern

Wenn Sie die LDAP-Authentifizierung nicht aktivieren, müssen Sie eine Auswahl treffen, wie Benutzer in Acrobat Connect Pro authentifiziert werden sollen.

Wenn Acrobat Connect Pro Benutzerinformationen aus einem externen Verzeichnis importiert, werden keine Netzwerkkennwörter importiert. Implementieren Sie deshalb eine andere Methode zum Verwalten der Kennwörter von Benutzern, die in das Acrobat Connect Pro-Verzeichnis importiert wurden.

Benutzer auffordern, ein Kennwort festzulegen

Im Bildschirm „Richtlinieneinstellungen“ der Registerkarte „Synchronisationseinstellungen“ können Sie festlegen, dass importierte Benutzer per E-Mail einen Link erhalten, über den sie ein Kennwort festlegen können.

Kennwort auf den Wert eines LDAP-Attributs einstellen

Sie können das anfängliche Kennwort eines importierten Benutzers auf den Wert eines Attributs im Verzeichniseintrag dieses Benutzers festlegen. Wenn das LDAP-Verzeichnis beispielsweise die Mitarbeiternummer als Feld enthält, können Sie das anfängliche Kennwort für Benutzer auf ihre jeweilige Mitarbeiternummer festlegen. Nachdem die Benutzer sich dann mit diesem Kennwort angemeldet haben, können sie ihre Kennwörter selbst ändern.

Empfohlene Verfahren für die Synchronisation

Als Administrator können Sie Acrobat Connect Pro auf zwei Arten mit dem externen LDAP-Verzeichnis synchronisieren:

- Sie können die Synchronisation planen, sodass sie in regelmäßigen Abständen ausgeführt wird.
- Sie können eine manuelle Synchronisation ausführen, bei der das Acrobat Connect Pro-Verzeichnis sofort mit dem LDAP-Verzeichnis der Organisation synchronisiert wird.

Bevor Sie Benutzer und Gruppen mit einer ersten Synchronisation importieren, überprüfen Sie am besten mithilfe eines LDAP-Browsers die Verbindungsparameter. Die folgenden Browser sind online verfügbar: LDAP Browser/Editor und LDAP Administrator.

Wichtig: *Starten Sie den LDAP-Server nicht neu und führen Sie während der Synchronisation keine anderen Vorgänge parallel aus. Dadurch könnten Benutzer oder Gruppen aus Acrobat Connect Pro gelöscht werden.*

Geplante Synchronisationen

Die Verwendung geplanter Synchronisationen wird empfohlen, da auf diese Weise gewährleistet ist, dass Acrobat Connect Pro immer über die aktuellen Daten der aus dem LDAP-Verzeichnis importierten Benutzer und Gruppen verfügt.

Wenn Sie eine große Anzahl an Benutzern und Gruppen importieren, erfordert die ursprüngliche Synchronisation möglicherweise eine erhebliche Menge an Kapazitäten. In diesem Fall sollten Sie diese erstmalige Synchronisation für einen Zeitpunkt außerhalb der Spitzenbelastungszeiten, zum Beispiel nachts, einplanen. (Alternativ dazu können Sie die Synchronisation zu einem geeigneten Zeitpunkt manuell ausführen.)

Um eine geplante Synchronisation einzurichten, verwenden Sie den Bildschirm „Synchronisationseinstellungen“ > „Planeinstellungen“ in der Anwendungsverwaltungskonsole.

Wenn eine Synchronisation stattfindet, vergleicht Acrobat Connect Pro die LDAP-Verzeichniseinträge mit den Einträgen im Acrobat Connect Pro-Verzeichnis und importiert nur die Einträge, in denen mindestens ein Feld geändert wurde.

Vorschau der Synchronisation anzeigen

Bevor Sie Benutzer und Gruppen in einer ersten Synchronisation importieren, wird empfohlen, die Zuordnungen zu überprüfen, indem Sie eine Vorschau der Synchronisation anzeigen. In einer Vorschau werden Benutzer und Gruppen nicht tatsächlich importiert, eventuelle Fehler werden jedoch protokolliert. Sie können diese Fehler untersuchen, um Probleme bei der Synchronisation zu vermeiden.

Über den Bildschirm „Synchronisationsprotokolle“ haben Sie Zugriff auf die Protokolle. Jede Zeile im Protokoll zeigt ein Synchronisationsereignis an. Bei der Synchronisation wird mindestens ein Ereignis für jedes verarbeitete Principal (Benutzer oder Gruppe) erzeugt. Falls bei der Vorschau Warnungen oder Fehler generiert werden, werden diese in einem zweiten Protokoll aufgezeichnet.

Werte in der Protokolldatei

Die Werte im Synchronisationsprotokoll werden durch Kommas getrennt gespeichert. In den folgenden Tabellen bezieht sich *Principal* auf Benutzer- und Gruppeneinträge. Die folgenden Werte sind in den Protokolleinträgen enthalten:

Feld	Beschreibung
Datum	Der formatierte Datum/Uhrzeit-Wert bis zur Millisekunde. Das Format ist *jjjjMMddTHHmmss.SSS*.
Principal-ID	Der Anmelde- oder Gruppenname.
Principal-Typ	Ein einzelnes Zeichen: U für Benutzer, G für Gruppe.
Ereignis	Die durchgeführte Aktion bzw. das festgestellte Problem.
Details	Detaillierte Informationen zum Ereignis.

In der folgenden Tabelle sind die verschiedenen Ereignisse aufgeführt, die in den Synchronisationsprotokollen vorkommen können:

Veranstaltung	Beschreibung	Details
add	Das Prinicipal wurde Acrobat Connect Pro hinzugefügt.	Ein gekürztes XML-Paket, dass die aktualisierten Felder durch eine Abfolge aus Tag-Paaren in folgendem Format beschreibt: **`<Feldname>Wert</Feldname>`** (beispielsweise, `<Vorname>Joe</Vorname>`). Die übergeordneten Knoten und die nicht aktualisierten Felder werden ausgelassen.
update	Das Principal ist ein externer Benutzer und einige Felder wurden aktualisiert.	

update-members	Das Principal ist eine externe Gruppe und Principals wurden der Gruppe hinzugefügt oder daraus entfernt.	Ein abgekürztes XML-Paket mit einer Beschreibung der hinzugefügten bzw. entfernten Mitglieder. Die übergeordneten Knoten werden ausgelassen:
		`<add>ID list</add>`
		`<remove>ID list</remove>`
		Bei der ID-Liste handelt es sich um mehrere `<id>Principal-ID</id>` -Pakete. Dabei entspricht `Principal-ID` der ID in der Spalte Principal-ID, wie z. B. ein Anmelde- oder ein Gruppenname. Falls es zu einer ID-Liste keine Mitglieder gibt, wird der übergeordnete Knoten als `<add/>` oder `<remove/>` ausgegeben.

delete	Das Principal wurde aus Acrobat Connect Pro gelöscht.	
up-to-date	Das Principal ist als externes Principal in Acrobat Connect Pro vorhanden und wurde bereits mit dem externen Verzeichnis synchronisiert. Dabei wurden keine Änderungen vorgenommen.	Bei einem in Acrobat Connect Pro erstellten Benutzer bzw. einer Gruppe wird von einem internen Principal gesprochen. Wird der Benutzer bzw. die Gruppe dagegen durch eine Synchronisation erstellt, handelt es sich um ein externes Principal.
make-external	Das Principal ist ein internes Principal in Acrobat Connect Pro und wurde in ein externes Principal konvertiert.	Dieses Ereignis ermöglicht die Änderung bzw. Löschung des Principals bei einer Synchronisation und geht daher normalerweise einem anderen Ereignis voraus, das eine dieser beiden Aufgaben bezeichnet. Dieses Ereignis wird im Warnungsprotokoll eingetragen.
warning	Ein Warnungsereignis ist eingetreten.	Eine Warnmeldung.
error	Ein Fehler ist aufgetreten.	Java-Ausnahmebenachrichtigung.

LDAPS

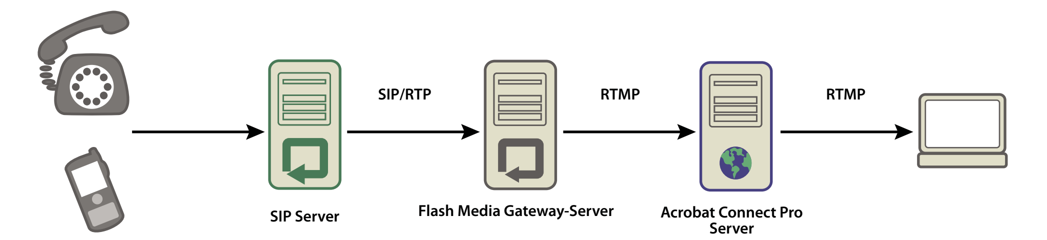
Acrobat Connect Pro unterstützt nativ das LDAP-Protokoll *LDAPS*. Der LDAP-Verzeichnisserver muss SSL-Konnektivität bieten. Um eine sichere Verbindung zu einem LDAP-Verzeichnisserver herzustellen, verwenden Sie das LDAPS-Protokoll in der Verbindungs-URL wie folgt: ldaps:// *Beispielverzeichnisserver* : *Portnummer* .

Bereitstellen von Universal Voice

Arbeitsablauf für das Bereitstellen von Universal Voice

Hinweis: *Eine Gegenüberstellung von Universal Voice und integrierten Telefonieadaptern finden Sie unter* *„Audiokonferenzoptionen mit Connect Pro“ auf Seite 14.*

Connect Pro Universal Voice verwendet eine Komponente mit dem Namen Flash Media Gateway, um Audiodaten von einem SIP-Server zu empfangen. Audio wird dabei nur in eine Richtung übertragen, nämlich vom SIP-Server an die Connect Pro-Meetingräume. Installieren Sie Flash Media Gateway und konfigurieren Sie die Software für die Kommunikation mit dem SIP-Server. Der SIP-Server kann von Dritten gehostet werden oder in die Infrastruktur Ihres Unternehmens eingegliedert sein. (SIP-Anbieter werden auch als *VoIP-Anbieter* bezeichnet.)



Die Audiodaten fließen vom Telefon über den Audiokonferenzserver (nicht dargestellt) durch den SIP-Server, und von dort durch Flash Media Gateway in einen Connect Pro-Meetingraum.

So implementieren Sie eine Universal Voice-Lösung:

1 Zum Installieren und Konfigurieren von Universal Voice benötigen Sie Folgendes:

- Connect Pro Server 7.5
- Anmeldeinformationen für SIP-Anbieter

2 Installieren Sie Flash Media Gateway.

Flash Media Gateway lässt sich auf demselben Server mit Connect Pro Server installieren oder auf einem dedizierten Computer. Flash Media Gateway lässt sich auf einem einzelnen Computer oder in einem Servercluster installieren. Das Installationsprogramm von Flash Media Gateway ist Teil des Connect Pro Server-Installationsprogramms. Weitere Informationen hierzu finden Sie unter „Ausführen des Installationsprogramms“ auf Seite 16.

3 Konfigurieren Sie Flash Media Gateway für die Verbindung mit einem SIP-Server.

Nach dem Abschluss der Installation wird die Anwendungsverwaltungskonsole gestartet. (Die Anwendungsverwaltungskonsole kann auch über http://localhost:8510/console aufgerufen werden.) Konfigurieren Sie Flash Media Gateway mithilfe der Konsole für die Verbindung mit einem SIP-Server. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Acrobat Connect Pro mit dem Assistenten der Anwendungsverwaltungskonsole“ auf Seite 18.

4 Öffnen Sie die benötigten Ports. Weitere Informationen hierzu finden Sie unter „Flash Media Gateway-Ports und -Protokolle“ auf Seite 42.

Falls die Firewall NAT verwendet, finden Sie weitere Informationen hierzu unter „Konfigurieren von Flash Media Gateway für die Kommunikation hinter einer Firewall mittels NAT“ auf Seite 42.

5 Weitere Informationen zur Installation von Flash Media Gateway auf einem Servercluster finden Sie unter„Bereitstellen von Flash Media Gateway auf einem Servercluster“ auf Seite 45.

6 Informationen zum Erstellen von Wählfolgen und zum Prüfen der Audioverbindung finden Sie unter www.adobe.com/go/learn_cnn_uvconfig_de.

7 Falls in einem Connect Pro-Meeting der Ton fehlt, finden Sie weitere Informationen hierzu unter „Fehlerbehebung bei Problemen mit Universal Voice“ auf Seite 46.

Flash Media Gateway-Ports und -Protokolle

Hinweis: *Ein Diagramm, das den Datenfluss zwischen SIP-Anbieter, Flash Media Gateway und Connect Pro Server beschreibt, finden Sie unter* *„Datenfluss“ auf Seite 8.*

Flash Media Gateway wartet auf Anfragen von Connect Pro Central Application Server auf folgendem Port:

Portnummer	Bind-Adresse	Protokoll
2222	*/Beliebiger Adapter	HTTP

Flash Media Gateway initiiert die Verbindung mit Flash Media Server wie ein normaler RTMP-Client. Flash Media Server wartet auf Flash Media Gateway auf folgendem Port:

Portnummer	Bind-Adresse	Protokoll
8506	*/Beliebiger Adapter	RTMP

Flash Media Gateway kommuniziert mit dem Audiokonferenzanbieter über die Protokolle SIP und RTP über folgende Ports:

Richtung	Regel
Flash Media Gateway zu Internet	SRC-IP=<Server-IP>, SRC-PORT=5060, DST-IP=ANY, DST-PORT=5060
Internet zu Flash Media Gateway	SRC-IP=ANY, SRC-PORT=5060, DST-IP=<Server-IP>, DST-PORT=5060
Flash Media Gateway zu Internet	SRC-IP=<Server-IP>, SRC-PORT=5000_TO_6000, DST-IP=ANY, DST-PORT=ANY_HIGH_END
Internet zu Flash Media Gateway	SRC-IP=ANY, SRC-PORT=ANY_HIGH_END, DST-IP=<Server-IP>, DST-PORT=5000_TO_6000

Hinweis: *ANY_HIGH_END bedeutet dabei eine beliebige Portnummer über 1024. Der Standardportbereich ist 5000 - 6000. Diese Werte lassen sich in der Anwendungsverwaltungskonsole ändern.*

Konfigurieren von Flash Media Gateway für die Kommunikation hinter einer Firewall mittels NAT

Hinweis: *Falls Ihre Firewall SIP-fähig ist oder für SIP eingerichtet wurde, muss dieser Task möglicherweise nicht ausgeführt werden. Möglicherweise führen auch die ALG (Application-Level Gateway) für SIP in einer Firewall zu Problemen. Falls Sie die erfolgreiche Kommunikation über ALG nicht herstellen können, sollte ALG für SIP in der Firewall deaktiviert und die im vorliegenden Abschnitt beschriebene Technik verwendet werden.*

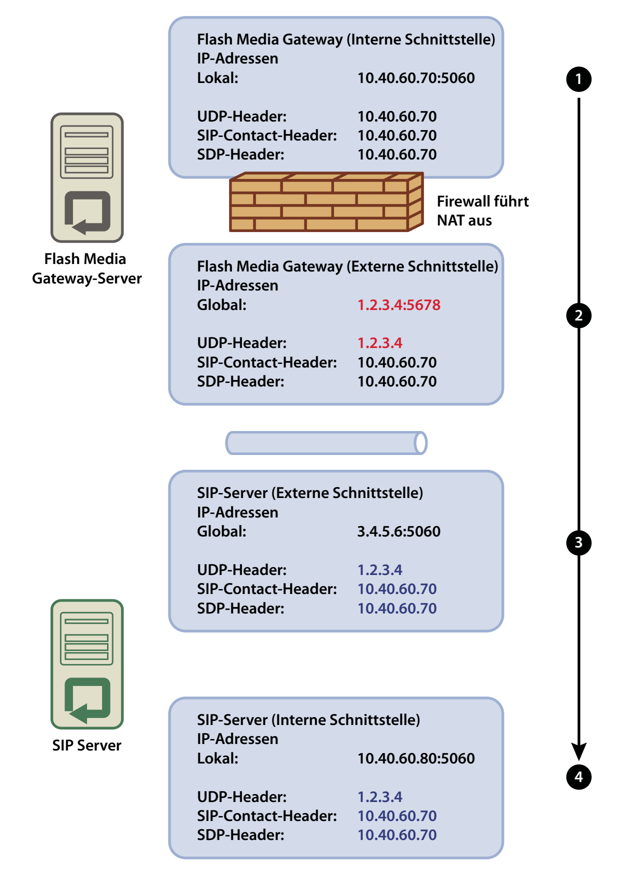
NAT (Network Address Translation) ist eine Technik, mit der Netzwerke weniger externe IP-Adressen benötigen und interne IP-Adressen verborgen werden. NAT ändert die IP-Adresse und die Portnummern von Paketen, die aus dem NAT-Netzwerk übertragen werden. Interne IP-Adressen werden in externe IP-Adressen umgewandelt. NAT versucht auch, Rückantworten an externe IP-Adressen an die zugehörigen internen IP-Adressen weiterzuleiten.

Wenn sich Flash Media Gateway hinter einer Firewall befindet, die NAT verwendet, kann die Software möglicherweise die Pakete des SIP-Servers nicht empfangen. NAT ändert lokale IP-Adressen und IP-Adressen im UDP-Header (Paketquelle) so, dass die Adressen den externen IP-Adressen entsprechen.

Die IP-Adresse im UDP-Header gleicht der externen IP-Adresse, die Flash Media Gateway verwendet. Flash Media Gateway erhält daher die nötige Rückantwort, wenn der SIP-Server für seine Antwort die IP-Adresse im UDP-Header verwendet.

Die IP-Adresse im Contact-Header gleicht der lokalen IP-Adresse des Flash Media Gateways. Flash Media Gateway kann daher die nötige Rückantwort nicht erhalten, wenn der SIP-Server für seine Antwort die IP-Adresse im SIP-Contact-Header verwendet. Lokale IP-Adressen sind hinter der Firewall verborgen und für den SIP-Server nicht sichtbar.

Die folgende Darstellung zeigt, wie NAT die IP-Adressen auf Firewall-Ebene ändert:



NAT ändert die IP-Adressen

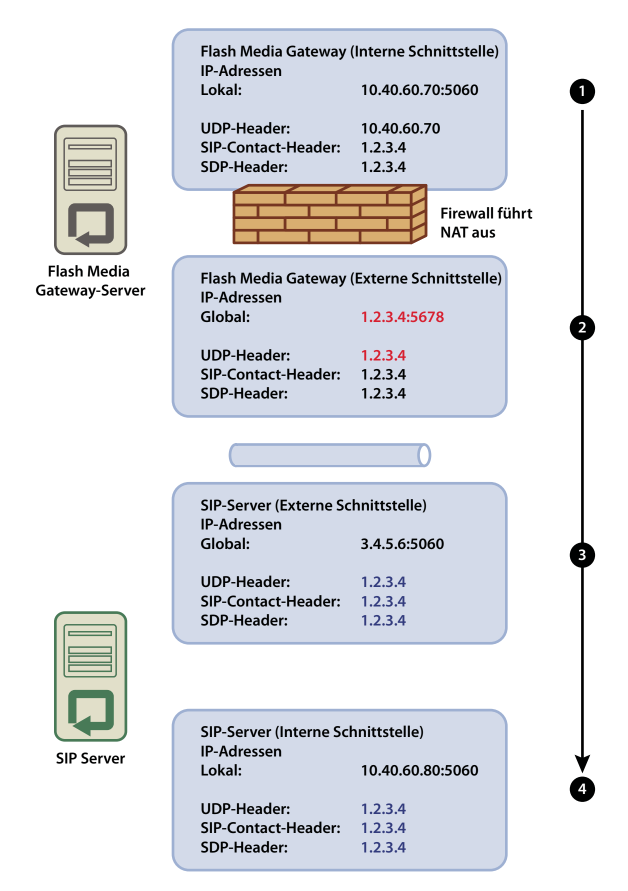
1 Flash Media Gateway (interne Schnittstelle). Die IP-Adressen des UDP-Headers (IP-Adresse der Paketquelle) und des SIP-Contact-Headers entsprechen der gleichen lokalen IP-Adresse.

2 Flash Media Gateway (externe Schnittstelle) NAT ändert die IP-Adresse des UDP-Headers in die globale IP-Adresse.

3 SIP-Server (externe Schnittstelle) Das Paket erreicht die globale Schnittstelle auf dem SIP-Server. Um die interne Schnittstelle erreichen zu können, muss der Port direkt weitergeleitet werden. Falls der Port nicht weitergeleitet wird, gehen die Pakete verloren und die Kommunikation bricht ab.

4 SIP-Server (interne Schnittstelle) Das Paket wird beim Erreichen der Schnittstelle weitergeleitet. Falls der SIP-Server die IP-Adresse des UDP-Headers verwendet, um eine Rückantwort zu senden, erreicht diese erfolgreich Flash Media Gateway. Falls der SIP-Server die IP-Adresse des Contact-Headers verwendet, kann die Rückantwort Flash Media Gateway nicht erreichen.

Folgende Darstellung zeigt eine erfolgreiche Konfiguration, in welcher die IP-Adresse des SIP-Contact-Headers die gleiche ist wie die externe IP-Adresse von Flash Media Gateway. Diese Änderung ermöglicht es den Paketen, vom SIP-Server zurück zu Flash Media Gateway geroutet zu werden.



Eine Konfiguration mit erfolgreicher Kommunikation

Mit folgenden Schritten stellen Sie sicher, dass Flash Media Gateway erfolgreich Pakete von einem SIP-Server empfangen kann:

1 Öffnen Sie auf dem Flash Media Gateway-Server die Datei *Stamm-Installationsverzeichnis*/conf/sip.xml in einem Texteditor. (Das Standardstammverzeichnis der Installation ist C:\Programme\Adobe\Flash Media Gateway.)

a Erstellen Sie das Tag `<globalAddress>` unter dem Tag `<Profile>`. Geben Sie die externe IP-Adresse des Flash Media Gateways ein, wie im folgenden Beispiel:

```
...
<Profiles>
    <Profile>
        <profil e I D>   s ipGateway </profileID>
        <userName>141583220 00 </ userName>
        <password></password>
        <displayName> sipGateway </displayName>
        <registrarAddress>8.15.247.100:5060</registrarAddress>
        <doRegister>0</doRegister>
        <defaulthost>8.15.247.100:5060</defaulthost>
        <hostPort> 0 </hostPort>
        <context> sipGatewayContext </context>
        <globalAddress>8.15.247.49</globalAddress>
        <supportedCodecs><codecID> G711u </codecID><codecID> speex </codecID>
    </supportedCodecs>
    </Profile>
</Profiles>
...
```

In einem Cluster muss jeder Flash Media Gateway-Server eine eindeutige externe IP-Adresse besitzen.

Wichtig: *Falls die externe IP-Adresse dynamisch ist, müssen Sie Flash Media Gateway jedesmal neu konfigurieren, wenn sich die externe IP-Adresse ändert.*

b Starten Sie den Dienst „Flash Media Gateway“ neu. Weitere Informationen hierzu finden Sie unter „Starten und Anhalten von Flash Media Gateway“ auf Seite 93

2 Leiten Sie auf der Firewall zwischen dem Flash Media Gateway-Server und dem SIP-Server den SIP-Port (Standardeinstellung: 5060) und alle RTP-Voice-Ports(Standardeinstellung: 5000 - 6000) direkt auf den Flash Media Gateway-Server weiter. Die auf der Firewall geöffneten Ports müssen den Ports entsprechen, die auf dem Flash Media Gateway-Server geöffnet sind.

Hinweis: *Die Server können ohne Port-Weiterleitung miteinander kommunizieren. Ohne Port-Weiterleitung kann es allerdings zu unerwarteten Verbindungsabbrüchen kommen, speziell nach langen Verbindungszeiten.*

Bereitstellen von Flash Media Gateway auf einem Servercluster

Installieren Sie Flash Media Gateway und Connect Pro Server jeweils auf dedizierten Computern, um einen Servercluster bereit zu stellen. Installieren Sie Connect Pro Server und Flash Media Gateway nicht auf denselben Computern.

Wenn Flash Media Gateway auf einem Servercluster installiert wird, übernimmt Connect Pro Server das Loadbalancing und das Failover. Connect Pro Edge Server erfordert keine weitere Konfiguration.

1 Starten Sie das Installationsprogramm auf jedem Server eines Clusters und wählen Sie die Installationsoption „Flash Media Gateway“. Weitere Informationen hierzu finden Sie unter „Ausführen des Installationsprogramms“ auf Seite 16.

Hinweis: *Weitere Informationen über das Bereitstellen von Connect Pro Server in einem Cluster finden Sie unter „Bereitstellen eines Clusters aus Acrobat Connect Pro-Servern“ auf Seite 25.*

2 Öffnen Sie auf einem Connect Pro-Server die Anwendungsverwaltungskonsole unter: http://localhost:8510/console/.

3 Wählen Sie „Flash Media Gateway-Einstellungen“ > „FMG-Host-Einstellungen“ und klicken Sie auf „Hinzufügen“, um zusätzliche Flash Media Gateway-Server hinzuzufügen und zu konfigurieren. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Acrobat Connect Pro mit dem Assistenten der Anwendungsverwaltungskonsole“ auf Seite 18.

Hinweis: *Geben Sie über die Anwendungsverwaltungskonsole eines Servers die Konfigurationsparameter für alle Server des Clusters ein. Die Anwendungsverwaltungskonsole übertragt die Konfigurationseinstellungen per Push an alle Server des Clusters.*

Erweiterte Konfigurationsoptionen für Flash Media Gateway

Informationen zu erweiterten Konfigurationsoptionen finden Sie unter Flash Media Gateway-Dokumentation.

Fehlerbehebung bei Problemen mit Universal Voice

Falls bei einer Universal Voice-Audiokonferenz in einem Meetingraum der Ton fehlt, gehen Sie wie folgt vor:

1 Achten Sie darauf, dass die Lautstärke auf dem Computer nicht stummgeschaltet ist. Achten Sie bei der Verwendung von Kopfhörern darauf, dass diese an der Ausgangsbuchse angeschlossen wurden.

2 Testen Sie die Wählfolge. Weitere Informationen hierzu finden Sie unter Testen von Wählfolgen.

3 Überprüfen der korrekten Konfiguration vonFlash Media Gateway:

  a Öffnen Sie die Anwendungsverwaltungskonsole (http://localhost:8510/console) unter Connect Pro Server und klicken Sie auf „Flash Media Gateway-Einstellungen“ > „FMG-Host-Einstellungen“. Der Status der einzelnen Flash Media Gateway-Instanzen muss „Aktiv“ sein.

  b Öffnen Sie die Datei *StammInstallationsVerzeichnis*/custom.ini, falls der Status nicht „Aktiv“ ist. Achten Sie darauf, dass folgende Einträge vorhanden sind:

```
FMG_ADMIN_USER=sa
FMG_ADMIN_PASSWORD=breeze
```

  Sollten diese Einträge nicht vorhanden sein, tragen Sie sie von Hand ein und starten Sie Connect Pro Central Application Server neu.

4 Wenden Sie sich an den Adobe-Support unter www.adobe.com/go/connect_licensed_programs_de.

Verwenden integrierter Telefonieadapter

Installieren integrierter Telefonieadapter

Integrierte Telefonieadapter sind Java-Erweiterungen, mit denen sich Connect Pro mit Audiobrücken verbinden kann. Es lassen sich beliebig viele integrierte Telefonieadapter installieren. Das Installationshandbuch ist unter folgender Adresse als Download erhältlich: Connect Pro-Hilfe- und Support-Center. Telefonieadapter erhalten Sie unter adobe.com.

Konfigurieren von Universal Voice für integrierte Telefonieadapter

Universal Voice lässt sich für die Nutzung mit beliebigen integrierten Telefonieadaptern konfigurieren, die auf Connect Pro Server installiert sind. Wenn ein integrierter Telefonieadapter für Universal Voice konfiguriert wurde, lässt sich eine Audiokonferenz an Teilnehmer des Meetingraums übertragen, wenn diese ausschließlich über VoIP an dem Meeting teilnehmen.

1 Öffnen Sie die Datei *Stamm-Installationsverzeichnis*\appserv\conf\telephony-settings.xml in einem Texteditor.

2 Legen Sie in der XML-Datei die Wählfolgen für die Audiokonferenzanbieter fest. Folgendes Beispiel nutzt die Wählfolge für den Premiere-Adapter:

Hinweis: *Dabei müssen Werte für die Parameter in eckigen Klammern ([]) eingegeben werden. Der Adapter stellt Werte für die Parameter in geschweiften Klammern ([]) bereit.*

```
 <telephony-adaptor  id="premiere-adaptor" class-name="com.macromedia.breeze_           e
xt.premiere.gateway.PTekGateway" enabled="true" name="{premiere-adaptor}" disable-
profiles-on-edit="false" disable-profiles-on-disable="false" default-recording-
source="adaptor">
    <setting id="PREMIERE_HOST">CSAXIS.PREMCONF .C OM </ se tt in g>
    <setting id="PREMIERE_PORT">443</setting>
    <setting id="PREMIERE_WEB_ID">[123456]</setting>
    <setting id="PREMIERE_PASSWORD">[aVerySecurePassword]</setting>
    <setting id="PREMIERE_MAX_DOWNLOAD_TRIES">120</setting>
    <setting id="PREMIERE_DOWNLOAD_LOGIN">[login]</setting>
    <setting id="PREMIERE_DOWNLOAD_PASSWORD">[aVerySecurePassword]</setting>
    <setting id="PREMIERE_REPORT_INTERVAL">60</setting>
    <setting id="PREMIERE_DOWNLOAD_URL">https://ww7.premconf.com/audio/</setting>
    <dial-in-sequence>
        <conf-num>{x-tel-premiere-conference-number}</conf-num>
        <delay>6000</delay>
        <dtmf>{x-tel-premiere-participant-code}</dtmf>
        <dtmf>#</dtmf>
        <delay>2000</delay>
        <dtmf>*#</dtmf>
        <delay>5000</delay>
    </dial-in-sequence>
</telephony-adaptor>
```

Folgendes Beispiel nutzt die Wählfolge für den InterCall-Adapter:

```
<telephony-adaptor id  ="intercall-adaptor" class-
name="com.macromedia.breeze_ext.telephony.Intercall.IntercallTelephonyAdaptor"
enabled="true" name="{intercall-adaptor}" disable-profiles-on-edit="false" disable-
profiles-on-disable="false" default-recording-source="audio-bridge">
    <setting
id="INTERCALL_CCAPI_HOST">https://iccapi.audiocontrols.net:8443/axis2/services/CCAPI</sett
ing>
    <setting
id="INTERCALL_CCAPI_AUTH_HOST">https://iccapi.audiocontrols.net:8443/axis2/services/Author
ization</setting>
    <setting id="INTERCALL_CLIENT_CALLBACK_URL">https://[external-
hostname]:8443/services/CCAPICallbackSOAP</setting>
    <setting id="INTERCALL_APP_TOKEN">[appTokenProvidedByIntercall]</setting>
    <setting id="INTERCALL_BREEZE_INSTALL">C:\breeze</setting>
    <dial-in-sequence><conf-num>{x-tel-intercall-conference-number}</conf-num>
<delay>6000</delay><dtmf>{x-tel-intercall-participant-code}</dtmf><dtmf>#</dtmf>
<delay>4000</delay><dtmf>#</dtmf><delay>8000</delay><dtmf>#</dtmf> </dial-in-
sequence></telephony-adaptor>
```

XML-Element	Beschreibung
conf-num	Die Rufnummer für die Einwahl in die Audiokonferenz. Dieses Element muss in der Wählfolge an erster Stelle stehen. Es darf nur ein einziges`<conf-num>`-Element vorhanden sein. Der Wert in geschweiften Klammern {} wird vom Adapter bereitgestellt.
Verzögerung	Eine Pause während der Wählfolge, in Millisekunden.
DTMF	Ein DTMF-Ton (Dual-Tone Multi Frequency). Ein DTMF-Wert kann eine beliebige Ziffer- oder Nummertaste auf dem Telefontastenfeld darstellen, einschließlich * und #.

3 Validieren und speichern Sie die XML-Datei.

4 Starten Sie Connect Pro Central Application Server neu.

Weitere Informationen über das Konfigurieren von Telefonieadaptern finden Sie unter *Verwenden von Telefonieadaptern* im Connect Pro-Hilfe- und Support-Center.

Ausblenden des Flash Media Gateway-Benutzers in der Teilnehmerliste

***Hinweis:** Dieser Abschnitt gilt nur für integrierte Telefonieadapter, die für Universal Voice konfiguriert wurden.*

Wenn sich ein Meetingraum mit Flash Media Gateway verbindet, wird diese Verbindung in Form eines Benutzer in der Teilnehmerliste angezeigt. Um den Flash Media Gateway-Benutzer in der Teilnehmerliste auszublenden, müssen Sie die Audiokonferenznummer in der Datei „custom.ini“ konfigurieren. Verwenden Sie für alle Computer eines Clusters dieselbe Nummer. Sie erhalten die Audiokonferenznummer von Ihrem SIP-Anbieter. Die Nummer findet sich auch im Meetingraum, wenn der Kontoadministrator in Connect Pro Central einen Audioanbieter konfiguriert hat.

1 Öffnen Sie die Datei „\breeze\custom.ini“ in einem Texteditor.

2 Fügen Sie folgenden Parameter hinzu:

```
UV_NUMBER={audio_conference_telephone_number}

// Example:
UV_NUMBER=4155551212
```

3 Speichern und schließen Sie die Datei „custom.ini“.

4 Starten Sie den Server mit folgenden Schritte neu:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server “ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server “ > „Connect Pro Central Application Server starten“.

Konfigurieren von gemeinsamem Speicher

Informationen zum gemeinsamen Speicher

In der Anwendungsverwaltungskonsole können Sie Acrobat Connect Pro so konfigurieren, dass NAS- und SAN-Geräte verwendet werden, um Materialspeicher zu verwalten. Materialien sind alle in Acrobat Connect Pro veröffentlichten Dateien, zum Beispiel Kurse, SWF-, PPT- oder PDF-Dateien sowie archivierte Aufzeichnungen.

Nachstehend sind mögliche Konfigurationen für den gemeinsamen Speicher aufgeführt:

- Material wird nur auf das primäre externe Speichergerät kopiert und bei Bedarf in den Materialordner aller Acrobat Connect Pro-Server geladen. Altes Material wird aus den Materialordnern der einzelnen Server gelöscht, um bei Bedarf Platz für neue Materialien zu schaffen. Bei dieser Konfiguration werden Ressourcen auf dem Anwendungsserver frei, was besonders in großen Clustern hilfreich ist. (Geben Sie Werte in die Felder „Gemeinsamer Speicher“ und „Größe des Content-Caches“ ein.)
- Material wird auf alle Server und das primäre externe Speichergerät kopiert. Diese Konfiguration wird für kleinere Cluster empfohlen, es sei denn, Sie verfügen über viele Materialien, auf die unsystematisch zugegriffen wird. (Geben Sie einen Wert in das Feld „Gemeinsamer Speicher“ ein; lassen Sie das Feld „Größe des Content-Caches“ leer.)

Hinweis: *Wenn Sie einen Acrobat Connect Pro-Cluster verwenden und keine gemeinsamen Speichergeräte konfigurieren, arbeitet der Cluster im Full-Mirroring-Modus (auf Acrobat Connect Pro veröffentlichtes Material wird auf alle Server kopiert), und Material wird niemals automatisch von einem der Server gelöscht.*

Konfigurieren von gemeinsamem Speicher

Wenn Sie gemeinsamen Speicher für einen Acrobat Connect Pro-Server konfigurieren, befolgen Sie die Anweisungen in der ersten Aufgabe. Wenn Sie gemeinsamen Speicher für einen Cluster konfigurieren, befolgen Sie die Anweisungen in der ersten Aufgabe für einen Computer des Clusters und dann die Anweisungen in der zweiten Aufgabe für alle anderen Computer im Cluster.

Verwandte Themen

„Unterstützte Materialspeichergeräte“ auf Seite 4

„Bereitstellen eines Clusters aus Acrobat Connect Pro-Servern“ auf Seite 25

Konfigurieren von gemeinsamem Speicher

Acrobat Connect Pro sollte ohne gemeinsamen Speicher konfiguriert und auf einem Server ausgeführt werden, bevor Sie fortfahren.

1 Konfigurieren Sie einen freigegebenen Datenträger auf einem externen Speichergerät.

Wenn ein freigegebener Datenträger einen Benutzernamen und ein Kennwort hat, müssen alle freigegebenen Datenträger denselben Benutzernamen und dasselbe Kennwort verwenden.

2 (Optional) Wenn Sie einen vorhandenen Acrobat Connect Pro-Server für die Verwendung gemeinsamer Speicherdatenträger aktualisieren möchten, müssen Sie das Material von einem der vorhandenen Server auf den freigegebenen (gemeinsam genutzten) Datenträger kopieren.

a Stoppen Sie den Server („Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen und Connect Pro Meeting Server stoppen“).

b Kopieren Sie den Ordner *[Stamm-Installationsverzeichnis]*\content\7 auf den freigegebenen Datenträger, den Sie in Schritt 1 erstellt haben.

Auf einigen Computern in einem Cluster befinden sich möglicherweise zusätzliche Materialien. Acrobat Connect Pro kann diese Dateien nicht verwenden, aber wenn Sie sie zur Archivierung auf den freigegebenen Datenträger kopieren möchten, können Sie ein Skript schreiben und ausführen, das die Materialien auf allen Computern mit denen auf dem freigegebenen Datenträger vergleicht.

c Starten Sie Acrobat Connect Pro („Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“ und „Connect Pro Meeting Server starten“).

3 Wählen Sie in Acrobat Connect Pro „Start“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“, um das Fenster „Dienste“ zu öffnen, wählen Sie „Adobe Connect Enterprise Service“ und führen Sie die folgenden Schritte aus:

a Klicken Sie mit der rechten Maustaste und wählen Sie „Eigenschaften“.

b Wählen Sie die Registerkarte „Anmelden“.

c Wählen Sie „Dieses Konto“. Falls für den freigegebenen Datenträger Benutzername und Kennwort festgelegt wurden, geben Sie beides ein. Klicken Sie auf „Anwenden“.

4 Starten Sie Acrobat Connect Pro erneut (nur Anwendungsserver).

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

5 Öffnen Sie die Anwendungsverwaltungskonsole („Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Server 7 konfigurieren“).

6 Wählen Sie im Fenster „Anwendungseinstellungen“ die Registerkarte „Servereinstellungen“, scrollen Sie bis zum Abschnitt „Einstellungen für gemeinsamen Speicher“ und geben Sie einen Ordnerpfad in das Feld „Gemeinsamer Speicher“ ein (zum Beispiel **storage**).

Wenn das primäre Speichergerät belegt ist, können Sie ein anderes Gerät an der primären Position hinzufügen. Trennen Sie die Pfade durch Semikolons (;):**new-storage;\\storage**.

Hinweis: *Das Schreiben (Kopieren in den Speicherordner) wird nur im ersten Ordner ausgeführt. Das Lesen (Kopieren aus dem Speicherordner) wird ab dem ersten Ordner in der entsprechenden Reihenfolge ausgeführt, bis die Datei gefunden wird.*

7 (Optional) Um den Materialordner auf Acrobat Connect Pro als Cache zu konfigurieren (Assets werden automatisch entfernt, wenn Speicherplatz benötigt wird, und auf Anforderung wiederhergestellt), geben Sie einen Wert im Feld „Größe des Content-Caches“ ein.

Dies ist ein prozentualer Anteil des Festplattenspeicherplatzes, der als Cache verwendet wird. Adobe empfiehlt, diesen Wert auf eine Zahl zwischen 15 und 50 zu setzen, da der Cache schnell über die eingestellte Größe hinauswachsen kann. Der Cache wird erst gelöscht, nachdem angezeigte Materialien abgelaufen sind (24 Stunden nach dem letzten Anzeigen).

8 Klicken Sie auf „Speichern“ und schließen Sie die Anwendungsverwaltungskonsole.

9 Starten Sie Acrobat Connect Pro erneut (nur Anwendungsserver).

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

Konfigurieren von gemeinsamem Speicher für zusätzliche Server in einem Cluster

1 Installieren Sie Acrobat Connect Pro, aber starten Sie das Programm nicht. Wenn Acrobat Connect Pro bereits installiert wurde und ausgeführt wird, beenden Sie das Programm.

2 Wählen Sie in Acrobat Connect Pro „Start“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“, um das Fenster „Dienste“ zu öffnen, wählen Sie „Adobe Connect Enterprise Service“ und führen Sie die folgenden Schritte aus:

a Klicken Sie mit der rechten Maustaste und wählen Sie „Eigenschaften“.

b Wählen Sie die Registerkarte „Anmelden“.

c Wählen Sie „Dieses Konto“. Falls für den freigegebenen Datenträger Benutzername und Kennwort festgelegt wurden, geben Sie beides ein. Klicken Sie auf „Anwenden“.

3 Starten Sie Acrobat Connect Pro.

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Server 7“ > „Adobe Connect Meeting Server starten“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

4 (Optional) Wenn Sie Acrobat Connect Pro zum ersten Mal installieren, befolgen Sie die Schritte unter „Bereitstellen eines Clusters aus Acrobat Connect Pro-Servern“ auf Seite 25.

5 Klicken Sie auf „Speichern“ und schließen Sie die Anwendungsverwaltungskonsole.

Konfigurieren von Kontobenachrichtigungseinstellungen

Hinzufügen von Support- und Statusverknüpfungen im Hilfemenü

Kontoadministratoren können dem Hilfemenü in Meetingräumen eine Statusseitenverknüpfung und eine Supportseitenverknüpfung hinzufügen. Die Verknüpfungen beziehen sich auf HTML-Seiten, die von Ihnen erstellt werden. Die Statusseite könnte beispielsweise Informationen über den aktuellen Zustand des Acrobat Connect Pro-Systems bieten. Auf der Supportseite könnten Informationen über verfügbare Hilfestellung zu Acrobat Connect Pro zusammengefasst sein. Diese Verknüpfungen sind nur im Hilfemenü verfügbar, wenn sie auch definiert wurden.

1 Öffnen Sie die Datei *StammInstallationsOrdner*\custom.ini in einem Texteditor.

2 Die Zuweisung `STATUS_PAGE = "http://connect.mycompany.com/status.html"` definiert die Statusseitenverknüpfung.

3 Die Zuweisung `SUPPORT_PAGE="http://connect.mycompany.com/support.html"` definiert die Supportseitenverknüpfung.

Die URLs können absolut oder relativ zur Domäne des Meetingsservers sein. Beginnin Sie absolute URLs mit „http://“ oder „https://“. Beginnen Sie relative URLs mit „/“

4 Führen Sie folgende Schritte aus, um Acrobat Connect Pro neu zu starten:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

Einstellen des Zeitpunkts, zu dem monatliche Berichte gesendet werden

Acrobat Connect Pro versendet eine monatliche E-Mail über die Kapazität Ihres Kontos. Standardmäßig werden die monatlichen Berichte über die Kontokapazität um 3:00 Uhr UTC versendet. Wenn Sie möchten, dass Acrobat Connect Pro die E-Mail zu einer anderen Zeit versendet, können Sie der Datei „custom.ini“ Parameter hinzufügen und die gewünschten Werte einstellen.

Weitere Informationen zur Konfiguration von Kontobenachrichtigungen in Acrobat Connect Pro Central finden Sie im Kapitel „Acrobat Connect Pro verwalten“ in „*Adobe Acrobat Connect Pro 7.5 nutzen*“ online unter www.adobe.com/go/connect_documentation_de.

1 Öffnen Sie die Datei *Stamm-Installationsverzeichnis*\custom.ini und fügen Sie der Datei die folgenden Parameter mit den gewünschten Werten hinzu:

THRESHOLD_MAIL_TIME_OF_DAY_HOURS Die Stundenzeit (UTC), zu der der monatliche Bericht zur Kapazitätsbenachrichtigung versendet wird. Bei diesem Wert muss es sich um eine Ganzzahl von 0 bis 23 handeln. Dieser Parameter kann nur in der Datei „custom.ini“ eingestellt werden. Eine Einstellung in Acrobat Connect Pro Central ist nicht möglich.

THRESHOLD_MAIL_TIME_OF_DAY_HOURS Die Minutenzeit (UTC), zu der der monatliche Bericht zur Kapazitätsbenachrichtigung versendet wird. Bei diesem Wert muss es sich um eine Ganzzahl von 0 bis 59 handeln.

Dieser Parameter kann nur in der Datei „custom.ini“ eingestellt werden. Eine Einstellung in Acrobat Connect Pro Central ist nicht möglich.

Hinweis: *Wenn einer dieser beiden Parameter nicht angegeben oder nicht korrekt angegeben wird, wird die E-Mail um 3:00 Uhr (UTC) versendet.*

Die folgenden Werte sind Beispielwerte, die zur „custom.ini“-Datei hinzugefügt wurden:

```
THRESHOLD_MAIL_TIME_OF_DAY = 5
THRESHOLD_MAIL_TIME_OF_MINUTES = 30
```

2 Führen Sie folgende Schritte aus, um Acrobat Connect Pro neu zu starten:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

Einrichten von Kapazitätsschwellenwerten

Acrobat Connect Pro-Benutzerkontoadministratoren können Kapazitätsschwellenwerte in Connect Pro Central einrichten. Wird dieser Schwellenwert im Konto überschritten, wird eine Benachrichtigung versendet. Sie können in der Datei „custom.ini“ Parameter hinzufügen, um die Standardkapazitätsschwellenwerte in Connect Pro Central festzulegen.

Weitere Informationen zur Konfiguration von Kontobenachrichtigungen in Acrobat Connect Pro Central finden Sie im Kapitel „Acrobat Connect Pro verwalten“ in *„Adobe Acrobat Connect Pro 7.5 nutzen“* online unter www.adobe.com/go/connect_documentation_de.

1 Öffnen Sie die Datei *Stamm-Installationsverzeichnis*\custom.ini und fügen Sie der Datei bei Bedarf folgende Parameter mit den gewünschten Werten hinzu.

THRESHOLD_NUM_OF_MEMBERS Der standardmäßige Schwellenwertprozentsatz für den Anteil an Autoren und Meetingveranstaltern. Dieser Wert muss eine Ganzzahl von 10 bis 100 und durch 10 teilbar sein. Wird dieser Wert nicht oder nicht korrekt eingegeben, wird der Wert auf 80 gesetzt.

THRESHOLD_CONC_USERS_PER_MEETING Der standardmäßige Schwellenwertprozentsatz für den Anteil an gleichzeitigen Benutzern pro Meeting. Dieser Wert muss eine Ganzzahl von 10 bis 100 und durch 10 teilbar sein. Wird dieser Wert nicht oder nicht korrekt eingegeben, wird der Wert auf 80 gesetzt.

THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT Der standardmäßige Schwellenwertprozentsatz für den kontoweiten Anteil an Meetingteilnehmern. Dieser Wert muss eine Ganzzahl von 10 bis 100 und durch 10 teilbar sein. Wird dieser Wert nicht oder nicht korrekt eingegeben, wird der Wert auf 80 gesetzt.

THRESHOLD_CONC_TRAINING_USERS Der standardmäßige Schwellenwertprozentsatz für den Anteil an gleichzeitigen Benutzern. Dieser Wert muss eine Ganzzahl von 10 bis 100 und durch 10 teilbar sein. Wird dieser Wert nicht oder nicht korrekt eingegeben, wird der Wert auf 80 gesetzt.

Die folgenden Werte sind Beispielwerte, die zur „custom.ini“-Datei hinzugefügt wurden:

```
THRESHOLD_NUM_OF_MEMBERS = 90
THRESHOLD_CONC_USERS_PER_MEETING = 90
THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT = 90
THRESHOLD_CONC_TRAINING_USERS = 75
```

2 Führen Sie folgende Schritte aus, um Acrobat Connect Pro neu zu starten:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

Konfigurieren einer PDF-zu-SWF-Konvertierung

Informationen zur PDF-Konvertierung

Zur Weitergabe von PDF-Dokumenten können Sie das Freigabe-Pod im Connect Pro-Meetingraum nutzen. Veranstalter und Moderatoren können die Navigation für alle Teilnehmer synchronisieren und mithilfe des Whiteboard-Overlays zusammenarbeiten. PDF-Dokumente lassen sich vom Desktop oder aus der Connect Pro-Inhaltebibliothek in das Freigabe-Pod kopieren. Die Weitergabe von Dokumenten im Freigabe-Pod bietet gegenüber der Bildschirmfreigabe folgende Vorteile:

- Veranstalter und Moderatoren können die Dokumente bereits im Vorfeld im Meetingraum laden und organisieren.
- Die Anzeigequalität ist für alle Teilnehmer höher.
- Die Bandbreitenanforderung für Teilnehmer und Moderatoren ist geringer.
- Die Zusammenarbeit mehrerer Moderatoren wird vereinfacht.
- Die Zusammenarbeit über das Whiteboard wird vereinfacht.

Wenn PDF-Dokumente über das Freigabe-Pod weitergegeben werden, konvertiert Connect Pro die Dateien in das Flash-Format. Connect Pro bietet Konfigurationsparameter zur Steuerung der PDF-Umwandlung.

Konfigurieren der PDF-zu-SWF-Umwandlung

1 Öffnen Sie die Datei *StammInstallationsOrdner*\custom.ini in einem Texteditor.

2 Bearbeiten Sie bei Bedarf folgende Konfigurationsparameter:

Parameter	Standardwert	Beschreibung
`ENABLE_PDF2SWF`	true	Ein boolescher Wert, der festlegt, ob die PDF-zu-SWF-Umwandlung für den Server aktiviert oder deaktiviert ist. Setzen Sie diesen Parameter auf „Falsch“, um die Umwandlung aus Gründen der Systemleistung zu deaktivieren.
`PDF2SWF_PAGE_TIMEOUT`	5	Der Timeout-Wert in Sekunden.
`PDF2SWF_CONVERTER_PORTS_START`	4000	Die niedrigste Portnummer des Portbereichs, der für die PDF-zu-SWF-Umwandlung genutzt wird.
`PDF2SWF_CONVERTER_PORTS_END`	4030	Die höchste Portnummer des Portbereichs, der für die PDF-zu-SWF-Umwandlung genutzt wird.
`PDF2SWF_CONCURRENCY_LIMIT`	3	Die maximale Anzahl gleichzeitiger PDF-zu-SWF-Umwandlungen, die auf einem Anwendungsserver stattfinden dürfen. Falls ein Anwendungsserver weitere Anfragen erhält, werden diese in einer Warteschlange gespeichert.

Parameter	Standardwert	Beschreibung
`PDF2SWF_QUEUE_LIMIT`	5	Die maximale Anzahl der PDF-zu-SWF-Umwandlungen, die gleichzeitig in einer Warteschlange vorhanden sein dürfen. Falls ein Anwendungsserver weitere Anfragen erhält, sieht der Benutzer die Nachricht „Connect Pro konnte die Datei nicht für die Anzeige konvertieren, bitte versuchen Sie es später erneut." Administratoren sehen in den Protokolldateien: <status code="request-retry"><exception>java.lang.Exception: Conversion Load too much on server.
`PDF2SWF_TIMEOUT_NUMBER_OF_PAGES`	3	Die maximale Anzahl der Seiten, für die ein Zeitüberlauf stattfinden darf, bevor die Umwandlung abgebrochen wird.

3 Starten Sie Connect Pro Central Application Server neu. Weitere Informationen hierzu finden Sie unter „Starten und Beenden von Acrobat Connect Pro Server" auf Seite 91

Integrieren mit Microsoft Live Communications Server 2005 und Microsoft Office Communications Server 2007

Arbeitsablauf für die Konfiguration der Presence-Integration

Integrieren Sie Acrobat Connect Pro mit einem Echtzeit-Kommunikationsserver von Microsoft, damit Meetingveranstalter die LCS- oder OCS-Präsenz registrierter Meetingteilnehmer in der Liste eingeladener Personen sehen können und textbasierte Unterhaltungen mit Onlinebenutzern führen können.

Informationen zur Liste eingeladener Personen finden Sie unter *„Adobe Acrobat Connect Pro nutzen"* online unterwww.adobe.com/go/connect_documentation_de.

1. Stellen Sie sicher, dass Acrobat Connect Pro Server und ein Kommunikationsserver installiert sind.

Installieren Sie Acrobat Connect Pro Server und einen Kommunikationsserver und bestätigen Sie die Installation. Acrobat Connect Pro Server unterstützt die Integration mit Microsoft Live Communications Server 2005 und Microsoft Office Communications Server 2007. Weitere Informationen hierzu finden Sie unter „Installieren von Connect Pro Server und Flash Media Gateway" auf Seite 16 und in der Dokumentation des Kommunikationsservers.

2. Konfigurieren Sie den Kommunikationsserver.

Konfigurieren Sie den Kommunikationsserver für den Datenaustausch mit Acrobat Connect Pro Server. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Live Communications Server 2005 oder Office Communications Server 2007" auf Seite 55.

3. Beenden Sie Connect Pro Presence Service.

Acrobat Connect Pro Server beinhaltet Connect Pro Presence Service. Beenden Sie den Dienst, bevor Sie Acrobat Connect Pro konfigurieren. Weitere Informationen hierzu finden Sie unter „Starten und Beenden von Connect Pro Presence Service" auf Seite 59.

4. Konfigurieren Sie Connect Pro Presence Service.

Konfigurieren Sie Acrobat Connect Pro so, dass Daten mit dem Kommunikationsserver ausgetauscht werden können. Der Präsenzserver wird in folgendes Verzeichnis installiert: *Stamm-Installationsverzeichnis*\presserv. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Connect Pro Presence Service" auf Seite 56.

5. Starten Sie Connect Pro Presence Service.

Weitere Informationen finden Sie unter „Starten und Beenden von Connect Pro Presence Service“ auf Seite 59.

6. Aktivieren Sie die Teilnehmerliste und den Chat-Pod in Connect Pro Central

Melden Sie sich als Administrator bei Connect Pro Central an. Wählen Sie „Administration“ > „Richtlinieneinhaltung und Kontrolle“ > „Pod-Verwaltung“. Wählen Sie die Option, die Teilnehmerliste und das Chat-Pod zu deaktivieren, ab.

Konfigurieren von Live Communications Server 2005 oder Office Communications Server 2007

1 Wählen Sie „Start“ > „Programme“ > „Verwaltung“ > „Live Communications Server 2005“ oder „Office Communications Server 2007“, um die Konfigurationskonsole zu öffnen.

2 Klicken Sie mit der rechten Maustaste auf den Wald, wählen Sie „Eigenschaften“ und gehen Sie wie folgt vor:

a Wählen Sie die Registerkarte „Verbund“ aus.

b Aktivieren Sie das Kontrollkästchen „Verbund und Verbindung mit öffentlichen Instant Messaging-Diensten aktivieren“ bzw. „Föderation und öffentliche IM-Verbindung aktivieren“.

c Geben Sie die Acrobat Connect Pro-Netzwerkadresse ein.

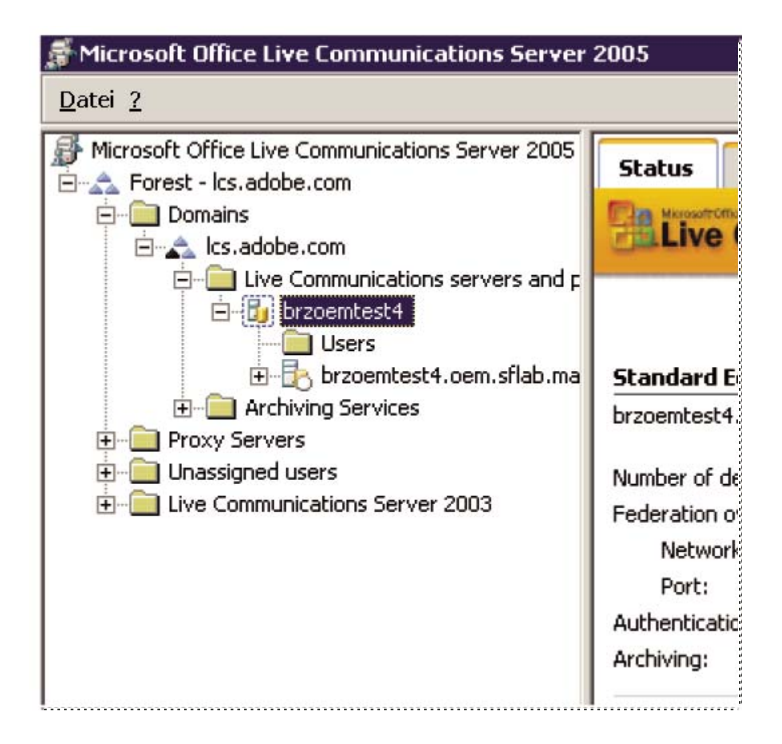
d Geben Sie Port 5072 ein.

5072 ist die Standardportnummer von Connect Pro Presence Service in der Datei „\presserv\conf\lcsgw.xml“.

e Klicken Sie auf „OK“.

3 Erweitern Sie im linken Bereich der Konfigurationskonsole Ihre Domain und erweitern Sie Live Communications-Server und -Pools.

4 Klicken Sie mit der rechten Maustaste auf den Hostnamen Ihres Pools und wählen Sie „Eigenschaften“.



5 Gehen Sie im Dialogfeld für Servereigenschaften wie folgt vor:

a Wählen Sie die Schaltfläche „Hostautorisierung". Fügen Sie die IP-Adresse von Acrobat Connect Pro hinzu. Bestätigen Sie, dass „Nur Ausgang" auf „Nein" gestellt ist, „Als Server drosseln" auf „Ja" und „Als Authentifizierung behandeln" ebenfalls auf „Ja".

b Wenn vor Ihrem Acrobat Connect Pro-Server ein Load Balancer installiert wird, wählen Sie die IP-Adresse des Load Balancers.

c Klicken Sie auf „OK".

6 Erweitern Sie im linken Bereich der Konfigurationskonsole die FQDN Ihres Servers und wählen Sie „Anwendungen".

7 Führen Sie folgende Schritte aus:

a Klicken Sie auf „Einstellung für IM-URL-Filteranwendung". Schalten Sie im Dialogfeld „Eigenschaften" die Aktivierung aus. Wenn diese Einstellung aktiviert ist, können Meetingveranstalter keine URLs mit Instant Messages versenden.

8 Schließen Sie die Konfigurationskonsole.

Konfigurieren von Kommunikationsserver-Clients

Die Acrobat Connect Pro-Integration mit Kommunikationsservern von Microsoft arbeitet mit Standardclients von Microsoft Office Communicator 2005 (MOC 2005). Für die Clients ist keine gesonderte Konfigurierung erforderlich. Damit allerdings Meeting-URLs aus Connect in MOC 2005 angeklickt werden können, ändern Sie die Eigenschaft „Hyperlinks in Instant Messaging-Anwendungen zulassen" in der Verwaltungsvorlage des Communicators. Weitere Informationen finden Sie unter http://technet.microsoft.com/de-de/library/bb963959.aspx.

1 Wählen Sie „Start" > „Ausführen".

2 Geben Sie im Textfeld „Öffnen" „gpedit.msc" ein, um das Fenster „Gruppenrichtlinie" zu öffnen.

3 Klicken Sie, um „Computerkonfiguration" zu erweitern.

4 Klicken Sie, um „Administrative Vorlagen" zu erweitern.

5 Klicken Sie mit der rechten Maustaste auf „Microsoft Office Communicator-Richtlinieneinstellungen" und wählen Sie „Eigenschaften".

Hinweis: *Wenn im Ordner „Administrative Vorlagen" die Vorlage „Microsoft Office Communicator-Richtlinieneinstellungen" fehlt, fügen Sie sie hinzu. Suchen Sie im Client-Paket von Microsoft Office Communicator 2005 nach der Datei „Communicator.adm" und kopieren Sie sie nach „C:\WINDOWS\inf\". Klicken Sie im Fenster „Gruppenrichtlinie mit der rechten Maustaste auf „Administrative Vorlagen", klicken Sie auf „Vorlagen hinzufügen/entfernen" und dann auf „Hinzufügen". Suchen Sie die Datei und klicken Sie auf „Öffnen".*

Konfigurieren von Connect Pro Presence Service

Führen Sie die folgenden vier Vorgänge durch, um Connect Pro Presence Service für den Datenaustausch mit einem Kommunikationsserver zu konfigurieren. Starten Sie nach Abschluss der Konfiguration Connect Pro Central Application Server neu.

Definieren der Gateway-Verbindung zwischen Connect Pro Presence Service und dem Kommunikationsserver

1 Öffnen Sie die Datei *Stamm-Installationsverzeichnis*\presserv\conf\lcsgw.xml in einem XML-Editor.

2 Bearbeiten Sie die Datei wie folgt und ersetzen Sie die fettgedruckten Werte durch Ihre eigenen:

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
<block xmlns="accept:config:sip-lcsgw">
<service trace="off" name="lcsgw" id="internal.server">
<stack name="lcs">
<via/>
</stack>
<state type="enabled"/>
<host type="external">lcs.adobe.com</host>
<domain-validation state="false"/>
<binding name="connector-0" transport="tcp">
<port>5072</port>
<bind>10.59.72.86</bind> <!-- LCS server IP -->
<area>lcs.adobe.com</area> <!-- LCS domain -->
</binding>
</service>
</block>
</config>
```

Parameter	Beschreibung
`<Veranstalter>`	SIP-Realm von LCS- oder OCS-Benutzern
`<bind>`	IP-Adresse des LCS- oder OCS-Servers (oder Load Balancers
`<area>`	SIP-Realm von LCS- oder OCS-Benutzern

Konfigurieren der Datei „custom.ini“

1 Öffnen Sie die Datei *Stamm-Installationsverzeichnis* in einem Texteditor.

2 Geben Sie die folgenden Parameter und Werte ein:

Parameter	Wert
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Bei diesem Wert wird zwischen Groß- und Kleinschreibung unterschieden.
OPN_HOST	Die Netzwerkadresse des Connect Pro Presence Service (zum Beispiel „localhost“).
OPN_PORT	Der zwischen Acrobat Connect Pro und Connect Pro Presence Service genutzte Port. Der Standardwert (10020) muss mit dem Wert in der Datei *Stamm-Installationsverzeichnis*\presserv\conf\router.xml übereinstimmen. Verändern Sie diesen Wert nicht.
OPN_PASSWORD	Das zwischen Acrobat Connect Pro und Connect Pro Presence Service genutzte interne Token. Der Standardwert (geheim) muss mit dem Wert in der Datei *Stamm-Installationsverzeichnis*\presserv\conf\router.xml übereinstimmen. Verändern Sie diesen Wert nicht.
OPN_DOMAIN	Der Domänenname des Acrobat Connect Pro-Servers (Anwendungsserver). Connect Pro Presence Service nutzt diesen Namen zur Identifikation des Anwendungsservers. In einem Cluster muss jeder Anwendungsserver seinen eigenen Domänennamen haben.
MEETING_PRESENCE_POLL_INTERVAL	Host-Clients führen in regelmäßigen Abständen Umfragen auf dem Präsenzserver durch, um den Status der eingeladenen Personen abzufragen. Dieser Parameter legt die Anzahl der Sekunden zwischen den Umfragen fest. Der Standardwert ist 30. Verändern Sie diesen Wert nicht.

Die folgenden Einstellungen sind Beispieleinstellungen:

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=breeze01.com
```

Definieren des SIP-Gateways zu Connect Pro Presence Service

1 Öffnen Sie die Datei *Stamm-Installationsverzeichnis*\presserv\conf\router.xml in einem XML-Editor.

2 Bearbeiten Sie die Datei wie folgt und ersetzen Sie die fettgedruckten Werte durch Ihre eigenen:

```
<block xmlns="accept:config:xmpp-gateway">
...
<block xmlns="accept:config:sip-stack-manager">
<service trace="off">
<bind>10.133.192.75</bind> <!-- presence server machine IP -->
<state type="enabled"/></service></block>
```

Geben Sie im Tag `<bind>` die IP-Adresse des Hostcomputers für Acrobat Connect Pro ein. Wenn mehrere IP-Adressen aufgeführt werden, wählen Sie die externe oder interne IP-Adresse, die der entfernte LCS- oder OCS-Server zur Verbindung mit Acrobat Connect Pro nutzen kann.

3 Starten Sie Connect Pro Central Application Server neu.

Konfigurieren von Connect Pro Presence Service in einem Cluster

Führen Sie, wenn Sie Connect Pro in einem Cluster betreiben, Connect Pro Presence Service nur auf einem Computer im Cluster aus. Konfigurieren Sie Connect Pro Presence Server jedoch auf allen Computern im Cluster, sodass ein Austausch des Präsenzdatenverkehrs zwischen ihnen stattfinden kann.

1 Öffnen Sie in einem Texteditor die Datei „custom.ini" aus dem *Stamminstallationsverzeichnis*.

2 Geben Sie die folgenden Parameter und Werte ein:

Parameter	Wert
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Bei diesem Wert wird zwischen Groß- und Kleinschreibung unterschieden.
OPN_HOST	Der FQDN des Computers, auf dem Connect Pro Presence Service ausgeführt wird. Der Wert des OPN_HOST-Parameters ist auf jedem Computer innerhalb des Clusters gleich.
OPN_PORT	Der zwischen Acrobat Connect Pro und Connect Pro Presence Service genutzte Port. Der Standardwert (10020) muss mit dem Wert in der Datei *Stamm-Installationsverzeichnis*\presserv\conf\router.xml übereinstimmen. Verändern Sie diesen Wert nicht.

Parameter	Wert
OPN_PASSWORD	Das zwischen Acrobat Connect Pro und Connect Pro Presence Service genutzte interne Token. Der Standardwert (geheim) muss mit dem Wert in der Datei *Stamm-Installationsverzeichnis*\presserv\conf\router.xml übereinstimmen. Verändern Sie diesen Wert nicht.
OPN_DOMAIN	Die Domäne, die von Connect Pro Presence Service zur Identifizierung eines Connect Pro-Servers in einem Cluster verwendet wird. Jedem Computer in einem Cluster muss ein eindeutiger Wert zugeordnet sein. Für den OPN_DOMAIN-Parameter kann jeder beliebige Wert gewählt werden (z. B. presence.connect1, presence.connect2, connect 3), solange der Wert innerhalb des Clusters eindeutig ist.
MEETING_PRESENCE_POLL_INTERVAL	Host-Clients führen in regelmäßigen Abständen Umfragen auf dem Präsenzserver durch, um den Status der eingeladenen Personen abzufragen. Dieser Parameter legt die Anzahl der Sekunden zwischen den Umfragen fest. Der Standardwert ist 30. Verändern Sie diesen Wert nicht.

Die folgenden Einstellungen sind Beispieleinstellungen:

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=presence.connect1
```

3 Starten Sie Connect Pro Central Application Server neu.

Starten und Beenden von Connect Pro Presence Service

Connect Pro Presence Service vom Startmenü oder vom Fenster „Dienste“ aus starten oder beenden.

Connect Pro Presence Service vom Startmenü aus starten und beenden

❖ Führen Sie einen der folgenden Schritte aus:

- Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Pro Server 7“ > „Connect Pro Presence Service starten“
- Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Pro Server 7“ > „Connect Pro Presence Service stoppen“.

Starten und Beenden von Connect Pro Presence Service vom Fenster „Dienste“ aus.

1 Wählen Sie „Start“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“, um das Fenster „Dienste“ zu öffnen.

2 Wählen Sie „Acrobat Connect Pro Presence Service“ und klicken Sie auf „Starten, Beenden oder Neustarten des Dienstes“.

Konfigurieren von Single Sign-On (SSO)

Informationen zu Single Sign-On

Single Sign-On ist ein Mechanismus, über den ein Benutzer für alle Anwendungen authentifiziert wird, für die er in einem Netzwerk Zugriffsberechtigungen besitzt. Beim Single Sign-On wird ein Proxyserver zur Authentifizierung von Benutzern verwendet, sodass sie sich nicht bei Acrobat Connect Pro anmelden müssen.

Acrobat Connect Pro unterstützt folgende Anmeldeverfahren:

HTTP-Header-Authentifizierung Dazu konfigurieren Sie einen Authentifizierungs-Proxy, der die HTTP-Anforderung abfängt, die Anmeldedaten des Benutzers vom Header analysiert und an Acrobat Connect Pro weitergibt.

Microsoft NT LAN Manager (NTLM)-Authentifizierung Konfigurieren Sie Connect Pro für die automatische Authentifizierung von Clients durch einen Windows-Domänencontroller über das NTLMv1-Protokoll. Microsoft Internet Explorer unter Microsoft Windows kann die NTLM-Authentifizierung abwickeln, ohne dass der Benutzer seine Anmeldedaten eingeben muss.

Hinweis: *Mozilla Firefox-Clients können die NTLM-Authentifizierung vielleicht auch ohne Dialogabfrage durchführen. Weitere Informationen zur Konfiguration finden Sie unter Firefox-Dokument.*

Sie haben auch die Möglichkeit, einen eigenen Authentifizierungsfilter zu erstellen. Weitere Informationen erhalten Sie vom Adobe-Support.

Konfigurieren der HTTP-Header-Authentifizierung

Wenn die HTTP-Header-Authentifizierung konfiguriert ist, werden Acrobat Connect Pro-Anmeldeanforderungen an einen Agenten weitergeleitet, der sich zwischen dem Client und Acrobat Connect Pro befindet. Bei diesem Agenten kann es sich um einen Authentifizierungs-Proxy oder um eine Softwareanwendung handeln. Der Agent authentifiziert den Benutzer, fügt der HTTP-Anforderung einen weiteren Header hinzu und sendet die Anforderung an Acrobat Connect Pro. Unter Acrobat Connect Pro müssen Sie die Kommentarmarkierung eines Java-Filters entfernen und in der Datei „custom.ini“ einen Parameter konfigurieren, der den Namen des zusätzlichen HTTP-Headers angibt.

Verwandte Themen

„Starten und Beenden von Acrobat Connect Pro Server“ auf Seite 91

Konfigurieren der HTTP-Header-Authentifizierung unter Acrobat Connect Pro

Um die HTTP-Header-Authentifizierung zu ermöglichen, müssen Sie auf dem Computer, der Acrobat Connect Pro hostet, eine Java-Filterzuordnung und einen Header-Parameter konfigurieren.

1 Öffnen Sie die Datei „*[Stamm-Installationsverzeichnis]*\appserv\conf\WEB-INF\web.xml“ und führen Sie folgende Schritte aus:

a Entfernen Sie die Kommentarmarkierung der Java-Filterzuordnung „HeaderAuthenticationFilter“.

```
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

b Kommentieren Sie die Java-Filterzuordnung „NtlmAuthenticationFilter“ aus.

```
<!--
<filter-mapping>
    <filter-name>NtlmAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

2 Beenden Sie Acrobat Connect Pro:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Server 7“ > „Connect Pro Central Meeting Server stoppen“.

3 Fügen Sie die folgende Zeile in die Datei „custom.ini“ ein:

```
HTTP_AUTH_HEADER=header_field_name
```

Der Authentifizierungsagent muss der HTTP-Anforderung, die an Acrobat Connect Pro gesendet wird, einen Header hinzufügen. Der Name des Headers muss „*header_field_name*“ lauten.

4 Speichern Sie die Datei „custom.ini“ und starten Sie Acrobat Connect Pro neu:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Server 7“ > „Adobe Connect Meeting Server starten“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

Authentifizierungscode schreiben

Der Authentifzierungscode muss den Benutzer authentifizieren, dem HTTP-Header ein Feld mit der Benutzeranmeldung hinzufügen und eine Anforderung an Acrobat Connect Pro senden.

1 Geben Sie für den Wert des Header-Felds *header_field_name* gültige Acrobat Connect Pro-Benutzeranmeldedaten ein.

2 Senden Sie eine HTTP-Anforderung an Acrobat Connect Pro unter folgender URL:

```
http://connectURL/system/login
```

Der Java-Filter für Acrobat ConnectPro erfasst die Anfrage für den Header *header_field_name* und sucht nach einem Benutzer mit der im Header befindlichen ID. Wenn der Benutzer ermittelt werden kann, wird er authentifiziert und es wird eine Antwort gesendet.

3 Der HTTP-Inhalt der Acrobat Connect Pro-Antwort wird nach der Zeichenfolge „OK" durchsucht, um eine erfolgreiche Authentifizierung zu bestätigen.

4 Die Acrobat Connect Pro-Antwort wird auf Vorhandensein des Cookies BREEZESESSION analysiert.

5 Verweisen Sie den Benutzer auf die erforderliche Acrobat Connect Pro-URL und geben Sie den Cookie BREEZESESSION als Wert des session-Parameters folgendermaßen an:

```
http://connectURL?session=BREEZESESSION
```

***Hinweis:** In dieser Client-Sitzung müssen Sie den Cookie BREEZESESSION auch bei allen weiteren Acrobat Connect Pro-Anfragen angeben.*

HTTP-Header-Authentifizierung mit Apache konfigurieren

Im Folgenden wird eine Beispielimplementierung einer HTTP-Header-Authentifizierung beschrieben, bei der Apache als Authentifizierungsagent eingesetzt wird.

1 Installieren Sie Apache als Reverse-Proxy auf einem anderen Computer als Acrobat Connect Pro.

2 Wählen Sie „Start“ > „Programme“ > „Apache HTTP Server“ > „Configure Apache Server“ > „Edit the Apache httpd.conf Configuration file“ und führen Sie Folgendes aus:

a Entfernen Sie die Kommentarmarkierung der folgenden Zeile:

```
LoadModule headers_module modules/mod_headers.so
```

b Entfernen Sie die Kommentarmarkierung der folgenden drei Zeilen:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

c Fügen Sie die folgenden Zeilen am Ende der Datei hinzu:

```
RequestHeader append custom-auth "ext-login"
ProxyRequests Off
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
ProxyPass / http://hostname:[port]/
ProxyPassReverse / http://hostname:[port]/
ProxyPreserveHost On
```

3 Beenden Sie Acrobat Connect Pro:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Server 7“ > „Connect Pro Central Meeting Server stoppen“.

4 Fügen Sie auf dem Computer, der Acrobat Connect Pro hostet, die folgenden Codezeilen in die Datei „custom.ini“ ein (diese Datei befindet sich im Stamm-Installationsverzeichnis, standardmäßig c:\breeze):

```
HTTP_AUTH_HEADER=custom-auth
```

Der Parameter `HTTP_AUTH_HEADER` muss dem in den Proxy-Einstellungen konfigurierten Namen entsprechen. (In diesem Beispiel wurde er in Zeile 1 von Schritt 2c konfiguriert.) Der Parameter ist der zusätzliche HTTP-Header.

5 Speichern Sie die Datei „custom.ini“ und starten Sie Acrobat Connect Pro neu:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Server 7“ > „Adobe Connect Meeting Server starten“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

6 Öffnen Sie die Datei „*[Stamm-Installationsverzeichnis]*\appserv\conf\WEB-INF\web.xml“ und führen Sie folgende Schritte aus:

a Entfernen Sie die Kommentarmarkierung der Java-Filterzuordnung „HeaderAuthenticationFilter“.

```
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

b Kommentieren Sie die Java-Filterzuordnung „NtlmAuthenticationFilter“ aus.

```
<!--
<filter-mapping>
    <filter-name>NtlmAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

Konfigurieren der NTLM-Authentifizierung

NTLMv1 ist ein Authentifizierungsprotokoll, das in Microsoft Windows-Netzwerken Bestandteil des SMB-Netzwerkprotokolls ist. Mit NTLM kann ein Benutzer seine Identität einmalig von der Windows-Domäne prüfen lassen, um künftig auf Netzwerkressourcen wie Connect Pro zugreifen zu können. Um die Identität des Benutzers zu verifizieren, führt der Webbrowser automatisch eine Challenge-Response-Authentifizierung durch Connect Pro über den Domänencontroller aus. Falls dieser Mechanismus fehlschlägt, kann der Benutzer sich auch direkt bei Connect Pro anmelden. Single-Sign-on mit NTLMv1-Authentifizierung wird unter Windows nur von Internet Explorer unterstützt.

Hinweis: *Standardmäßig erfordern Windows Server 2003-Domänencontroller eine Sicherheitsfunktion, die SMB-Signatur genannt wird. SMB-Signaturen werden von der Standardkonfiguration des NTLM-Authentifizierungsfilters nicht unterstützt. Der Filter lässt sich aber für die genannte Funktionsweise entsprechend konfigurieren. Weitere Informationen über diese und andere erweiterte Konfigurationsoptionen finden Sie unter JCIFS NTLM HTTP authentication documentation.*

Konfigurationsparameter hinzufügen

Führen Sie für jeden Host eines Connect Pro-Clusters folgende Schritte durch:

1 Öffnen Sie die Datei *root_install_dir*\custom.ini in einem Texteditor und fügen Sie folgende Parameter hinzu:

```
NTLM_DOMAIN=[domain]
NTLM_SERVER=[WINS_server_IP_address]
```

Der Wert `[domain]` ist der Name der Windows-Domäne, deren Mitglieder die Benutzer sind und die für die Authentifizierung maßgeblich ist. Beispiel: FIRMENNETZ. Möglicherweise müssen Sie diesen Wert so ändern, dass der Domänenname mit Windows-Versionen vor Windows 2000 kompatibel ist. Weitere Informationen hierzu finden Sie unter TechNote 27e73404. Dieser Wert wird auf die Filtereigenschaft `jcifs.smb.client.domain` abgebildet. Durch das direkte Einstellen eines Wertes in der Datei web.xml wird der Wert aus der Datei custom.ini außer Kraft gesetzt.

Der Wert `[WINS_server_IP_address]` ist eine durch Kommas getrennte Liste mit IP-Adressen von WINS-Servern. Es müssen IP-Adressen eingegeben werden, der Hostname funktioniert nicht. Die WINS-Server werden in der angegebenen Reihenfolge abgefragt, um die IP-Adresse eines Domänencontrollers für die Domäne aufzulösen, die im Parameter `NTLM_DOMAIN` hinterlegt ist. (Der Domänencontroller authentifiziert die Benutzer.) Sie können auch direkt die Adresse des Domänencontrollers eingeben, beispielsweise: 10.169.10.77, 10.169.10.66. Dieser Wert wird auf die Filtereigenschaft `jcifs.netbios.wins` abgebildet. Durch das Einstellen des Wertes in der Datei web.xml wird der entsprechende Wert in der Datei custom.ini außer Kraft gesetzt.

2 Speichern Sie die Datei custom.ini.

3 Öffnen Sie die Datei *root_install_dir*\appserv\conf\WEB-INF\web.xml in einem Texteditor und führen Sie folgende Schritte durch:

a Entfernen Sie die Kommentarmarkierung der NtlmAuthenticationFilter-Abbildung, so dass sich folgender Text ergibt:

```
<filter-mapping>
    <filter-name>NtlmAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

b Setzen Sie die Kommentarmarkierung der NtlmAuthenticationFilter-Abbildung, so dass sich folgender Text ergibt:

```
<!--
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
-->
```

4 Speichern Sie die Datei web.xml.

5 Starten Sie Connect Pro neu.

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server “ > „Adobe Acrobat Connect Pro Server beenden“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server “ > „Adobe Acrobat Connect Pro Server starten“.

Anmelderichtlinien angleichen

Connect Pro und NTLM verwenden unterschiedliche Anmelderichtlinien für die Benutzerauthentifizierung. Diese Richtlinien müssen aufeinander abgestimmt werden, bevor die Benutzer die Single-Login-Funktion nutzen können.

Bei der Anmeldekennung des NTLM-Protokolls kann es sich je nach Richtlinie oder Unternehmen um einen Benutzernamen (gschmidt), eine Mitarbeiter-ID (1234) oder um einen verschlüsselten Namen handeln. Standardmäßig verwendet Connect Pro eine E-Mail-Adresse (gschmidt@meinefirma.com) als Anmeldekennung. Ändern Sie die Connect Pro-Anmelderichtlinie, so dass Connect Pro einen eindeutigen Bezeichner mit NTLM verwendet.

1 Öffnen Sie Connect Pro Central.

Um Connect Pro Central zu öffnen, öffnen Sie ein Browserfenster und geben Sie den vollständig qualifizierten Domänennamen des Connect Pro-Hosts ein (z. B. http://connect.beispielfirma.com). Den Wert für „Connect Pro Host“ haben Sie im Bildschirm „Servereinstellungen“ der Anwendungsverwaltungskonsole eingegeben.

2 Wählen Sie die Registerkarte „Administration“ aus. Klicken Sie auf „Benutzer und Gruppen“. Klicken Sie auf „Anmelde- und Kennwortrichtlinien bearbeiten“.

3 Wählen Sie im Bereich „Anmelderichtlinie“ für „E-Mail-Adresse für Anmeldung verwenden“ die Option „Nein“.

Konfigurieren eines vorgelagerten Reverse-Proxys für Connect Pro Server

Verwenden eines Reverse-Proxys

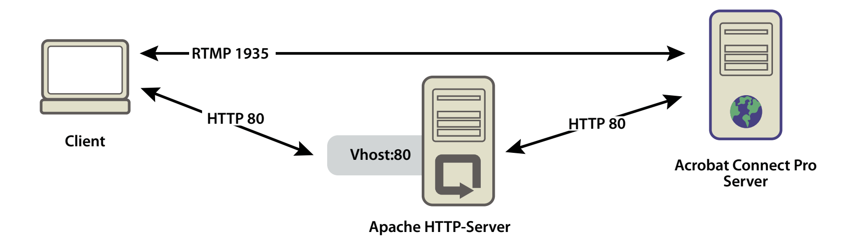
Es lässt sich ein Reverse-Proxy konfigurieren, der Connect Pro Server vorgelagert ist. Der Netzwerkverkehr fließt zunächst durch den Reverse-Proxy und erreicht dann erst Connect Pro Server. Verwenden Sie diese Konfiguration für folgende Zielsetzung:

- Connect Pro Server aus der DMZ ausgliedern.

  Den Reverse-Proxy in die DMZ aufnehmen und Connect Pro Server hinter der Firewall des Unternehmens betreiben.

- Benutzer vor der Nutzung von Connect Pro Server authentifizieren.

  Der Reverse-Proxy authentifiziert Benutzer über ein anderes System und berechtigt sie zur Verbindung mit Connect Pro Server.



HTTP-Netzwerkverkehr fließt zunächst durch den Apache HTTP-Server und erreicht dann erst Connect Pro-Server.

Konfigurieren eines Reverse-Proxys

Das folgende Beispiel verwendet eine Windows-Installation (32-Bit) des Apache HTTP-Servers. Die Konfiguration ist dabei für alle von Apache unterstützten Betriebssysteme identisch. In diesem Beispiel wird SSL nicht verwendet; der Netzwerkverkehr zum Connect Pro-Anwendungsserver bleibt unverschlüsselt.

Mit folgenden Schritten wird veranlasst, dass der gesamt HTTP-Verkehr zunächst durch den Apache HTTP-Server fließt, bevor er Connect Pro erreicht:

Hinweis: *RTMP-Verkehr wird in dieser Konfiguration nicht durch den Apache HTTP-Server geleitet.*

1 Installieren Sie den Apache HTTP-Server.

Standardmäßig befinden sich die Apache-Konfigurationsdateien unter c:\Programme\Apache Software Foundation\Apache2.2\conf\.

2 Konfigurieren Sie Apache, damit dieser den Netzwerkverkehr auf Port 80 aufgreift.

Öffnen Sie die Datei c:\Programme\Apache Software Foundation\Apache2.2\conf\httpd.conf in einem Texteditor und fügen Sie folgenden Text hinzu:

```
#
# Listen: Allows you to bind Apache to specific IP addresses and
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
#
#
```

3 Laden Sie die zum Betrieb des Reverse-Proxys erforderlichen Module.

Entfernen Sie in derselben Datei (httpd.conf) die Kommentarzeichen folgender Dateien.

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
```

4 Verknüpfen Sie die Datei httpd.conf mit der Konfigurationsdatei, mit der Verbindungen an Connect Pro weitergeleitet werden.

Fügend Sie als letzte Zeile der Datei httpd.conf folgenden Text hinzu:

```
Include conf/extra/httpd-connect.conf
```

5 Erstellen Sie eine Textdatei mit dem Namen httpd-connect.conf und speichern Sie diese unter c:\Programme\Apache Software Foundation\Apache2.2\conf\extra.

6 Fügen Sie der Datei httpd-connect.conf folgende Zeilen hinzu (setzen Sie an den erforderlichen Stellen Ihre IP-Adressen und Ports ein):

```
#vhost for application server
<VirtualHost *:80>
ProxyRequests Off
ProxyPreserveHost On
ProxyPass / http://<IP-of-Connect-Application-Server>:80/
ProxyPassReverse / http://<IP-of-Connect-Application-Server>:80/
ServerName <FQDN of Apache host>
</VirtualHost>
```

7 Speichern Sie die Datei und starten Sie den Apache-Dienst neu.

8 Öffnen Sie auf Connect Pro Server die Anwendungsverwaltungskonsole in einem Browser: http://localhost:8510/console/.

9 Nehmen Sie im Bildschirm „Servereinstellungen“ folgende Änderungen vor:

- Stellen Sie als Connect Pro-Host den FQDN des Apache HTTP-Servers ein.
- Setzen Sie „Externer Name“ auf den FQDN des Computers, auf dem Connect Meeting Server gehostet wird.

10 Starten Sie die Dienste „Adobe Connect Pro“ (den Anwendungsserver) und „Flash Media Server (FMS) neu. Weitere Informationen hierzu finden Sie unter „Starten und Beenden der Server“ auf Seite 91.

RTMP wird zu Connect Pro geroutet und HTTP wird durch Apache geleitet.

Hosting für Acrobat Connect-Add-In

Informationen zum Acrobat Connect-Add-In

Das Adobe Acrobat Connect-Add-In ist eine Version von Flash Player, die Acrobat Connect Pro mit zusätzlichen Funktionen ausstattet.

Wenn das Acrobat Connect-Add-In erforderlich ist, wird es automatisch von einem Adobe-Server heruntergeladen, ohne dass der Benutzer dies bemerkt. Wenn in Ihrem Unternehmen der Download von Software von externen Servern nicht zulässig ist, können Sie das Acrobat Connect-Add-In auch auf einem eigenen Server bereitstellen.

Meetinggäste, registrierte Benutzer und Moderatoren werden aufgefordert, das Acrobat Connect-Add-In herunterzuladen, wenn derzeit eine alte Version auf ihrem Computer installiert ist. Sie werden dann zum Veranstalter oder Moderator ernannt oder erhalten erweiterte Rechte für den Freigabe-Pod.

Meetingveranstalter müssen das Acrobat Connect-Add-In herunterladen, wenn es noch nicht vorhanden ist oder wenn eine ältere Version installiert ist.

Anpassen des Download-Speicherorts für das Connect-Add-In

Sie können das Acrobat Connect-Add-In auf Ihrem Server bereitstellen und Benutzer direkt zu den ausführbaren Dateien leiten. Als Alternative können Sie die Benutzer zu einer Seite mit Download-Anleitungen leiten, die Links zu den ausführbaren Dateien enthält. Sie können eine eigene Seite mit Download-Anleitungen erstellen oder eine von Adobe bereitgestellte Seite verwenden. Die Adobe-Seite steht in allen unterstützten Sprachen zur Verfügung.

Benutzer direkt zu den ausführbaren Dateien senden

1 Suchen Sie auf dem Server mit Acrobat Connect Pro die Acrobat Connect Pro-XML-Dateien für die Sprachen. Die XML-Dateien befinden sich in den folgenden zwei Verzeichnissen: *[Stamminstallationsverzeichnis]*\appserv\web\common\intro\lang und *[Stamminstallationsverzeichnis]*\appserv\web\common\meeting\lang\.

2 Geben Sie den Pfad der ausführbaren Dateien für jede Plattform im Abschnitt `addInLocation` jeder Plattform in jeder Sprachdatei ein:

```
<m id="addInLocation" platform="Mac OS 10">/common/addin/AcrobatConnectAddin.z</m>
<m id="addInLocation" platform="Windows">/common/addin/setup.exe</m>
```

Hinweis: *Dies sind die Standardspeicherorte der ausführbaren Dateien des Add-Ins. Sie können die Speicherorte auf Ihrem Server ändern und die Pfadangaben im Abschnitt* `addInLocation` *entsprechend anpassen.*

Benutzer zu von Adobe bereitgestellten Seiten mit Download-Anleitungen senden:

1 Suchen Sie auf dem Server mit Acrobat Connect Pro die Acrobat Connect Pro-XML-Dateien für die Sprachen. Die XML-Dateien befinden sich in den folgenden zwei Verzeichnissen:*[Stamminstallationsverzeichnis]*\appserv\web\common\intro\lang und *[Stamminstallationsverzeichnis]*\appserv\web\common\meeting\lang\.

2 Geben Sie dem Pfad zur Anweisungsseite zum Herunterladen im Abschnitt `addInLocation` jeder Plattform in jeder Sprachdatei ein:

```
<m id="addInLocation" platform="Mac OS 10">/common/help/#lang#/support/addindownload.htm</m>
<m id="addInLocation" platform="Windows">/common/help/#lang#/support/addindownload.htm</m>
```

Hinweis: *Der Pfad enthält die Zeichenfolge* `#lang#`*, die von Acrobat Connect Pro durch die Sprache des aktuellen Meetings ersetzt wird.*

3 Die addindownload.htm-Dateien enthalten Links zu den ausführbaren Add-In-Dateien an ihren Standardspeicherorten unter Acrobat Connect Pro (/common/addin/setup.exe und /common/addin/AcrobatConnectAddin.z). Wenn Sie die ausführbaren Dateien in einem anderen Verzeichnis speichern, aktualisieren Sie die Links auf der Seite „addindownload.htm" für jede Sprache.

Benutzer zu selbst erstellten Seiten mit Download-Anleitungen senden:

1 Suchen Sie auf dem Server mit Acrobat Connect Pro die Acrobat Connect Pro-XML-Dateien für die Sprachen. Die XML-Dateien befinden sich in den folgenden zwei Verzeichnissen:*[Stamminstallationsverzeichnis]*\appserv\web\common\intro\lang und *[Stamminstallationsverzeichnis]*\appserv\web\common\meeting\lang\.

2 Im Abschnitt `addInLocation` geben Sie den Pfad der von Ihnen erstellten Anleitungsseite für jede Plattform in jeder Sprachdatei ein:

```
<m id="addInLocation" platform="Mac OS 
10">common/help/#lang#/support/addin_install_instructions.html</m>
<m id="addInLocation" 
platform="Windows">common/help/#lang#/support/addin_install_instructions.html</m>
```

Hinweis: *Sie können für jede Plattform separate Anleitungsseiten erstellen.*

3 Erstellen Sie eine Anleitungsseite in jeder Sprache, die unterstützt werden soll. Fügen Sie auf der Anleitungsseite für jede Plattform Links zu den ausführbaren Add-In-Dateien ein.

Kapitel 4: Sicherheit

Durch Absichern von Adobe Acrobat Connect Pro Server schützen Sie Ihr Unternehmen vor Verlusten und böswilligen Angriffen. Es ist wichtig, dass die Infrastruktur Ihres Unternehmens, Acrobat Connect Pro und der von Acrobat Connect Pro genutzte Datenbankserver geschützt sind.

SSL (Secure Sockets Layer)

Informationen zur SSL-Unterstützung

Acrobat Connect Pro besteht aus zwei Servern: Adobe® Flash® Media Server und Acrobat Connect Pro-Anwendungsserver. Der Flash Media Server wird auch als *Meetingserver* bezeichnet, da er Meetings über eine Echtzeit-RTMP-Verbindung an den Client weitergibt. Der Acrobat Connect Pro-Anwendungsserver steuert die HTTP-Verbindung zwischen dem Client und der Acrobat Connect Pro-Anwendungslogik.

***Hinweis:** Im Startmenü wird der Meetingserver als „Connect Pro Meeting Server" bezeichnet, der Anwendungsserver als „Connect Pro Central Application Server". Im Fenster „Dienste" wird der Meetingserver als „Flash Media Server (FMS)" bezeichnet, der Anwendungsserver heißt „Adobe Connect Enterprise Service".*

Sie können SSL für den Anwendungsserver, für den Meetingserver oder für beide konfigurieren.

Hardwarebasierte Lösung Verwenden Sie einen SSL-Beschleuniger, um die zuverlässigste SSL-Konfiguration zu erzielen.

Einen SSL-Beschleuniger können Sie separat kaufen. Adobe hat die Funktionsfähigkeit von Acrobat Connect Pro mit den folgenden SSL-Hardwarebeschleunigern getestet: F5 Big-IP 1000, Cisco Catalyst 6590 Switch und Radware T100.

Softwarebasierte Lösung Verwenden Sie die native SSL-Unterstützung von Acrobat Connect Pro.

***Hinweis:** SSL wird unter Microsoft® Windows® 98 nicht unterstützt.*

Acrobat Connect Pro verwendet die HTTP-Methode CONNECT, um eine SSL-Verbindung anzufordern. Proxyserver müssen zulassen, dass Clients die Methode CONNECT verwenden. Wenn Clients die Methode CONNECT nicht nutzen können, tunneln RTMP-Verbindungen über HTTP/HTTPS.

Wenn Sie Hilfe bei der SSL-Konfiguration benötigen, wenden Sie sich an den Adobe-Support unter www.adobe.com/go/connect_licensed_programs_de.

Verwenden von Zertifikaten

Mit einem SSL-Zertifikat wird die Identität des Servers für den Client überprüft.

Um die Meetingserver-Verbindung (RTMP) und die Anwendungsserver-Verbindung (HTTP) zu sichern, benötigen Sie zwei SSL-Zertifikate, eines für jede Verbindung. Um SSL für einen Cluster von Computern, auf denen Acrobat Connect Pro gehostet wird, zu konfigurieren, benötigen Sie für jeden Meetingserver ein SSL-Zertifikat. Alle Anwendungsserver in einem Cluster können ein SSL-Zertifikat gemeinsam nutzen.

Beispiel: Zum Sichern der Meetingserver- und Anwendungsserver-Verbindungen auf einem Server benötigen Sie insgesamt zwei SSL-Zertifikate. Um die Meetingserver- und Anwendungsserver-Verbindungen in einem Cluster aus drei Servern zu schützen, benötigen Sie vier SSL-Zertifikate – eines für die Anwendungsserver und drei für die Meetingserver.

Zertifikate erhalten

❖ Wenden Sie sich an eine Zertifizierungsstelle. Dabei handelt es sich um einen vertrauenswürdigen Drittanbieter, der die Identität des Antragstellers überprüft. (Selbstsignierte Zertifikate funktionieren nicht mit Acrobat Connect Pro.)

Die Zertifizierungsstelle fordert Sie auf, eine SSL CSR-Datei zu generieren (CSR = Certificate Signing Request, Zertifikatsignierungsanfrage). Senden Sie die CSR an die Zertifizierungsstelle, die sie dann in ein SSL-Zertifikat konvertiert. Die Datei enthält Informationen über Ihre Organisation und den vollständig qualifizierten Domänennamen (fully qualified domain name, FQDN), der mit dem SSL-Zertifikat verknüpft ist. Anweisungen zum Generieren eines CSR erhalten Sie von der Zertifizierungsstelle.

Wichtig: *Speichern Sie die Kennwörter für Ihre SSL-Zertifikate an einem sicheren Ort, auf den Sie Zugriff haben.*

Zertifikate installieren

❖ Installieren Sie die SSL-Zertifikate im PEM-Format im Stammordner von Acrobat Connect Pro (standardmäßig c:\breeze).

Wenn Sie eine CRT-Datei von einer Zertifizierungsstelle erhalten, können Sie die Datei umbenennen; die Dateierweiterung muss.pem lauten.

Hinweis: *Für jede gesicherte Verbindung werden zwei Dateien benötigt: eine Datei für das öffentliche Zertifikat und eine zweite Datei für den zugehörigen privaten Schlüssel. Der Server sendet das öffentliche Zertifikat an den Client. Der private Schlüssen verbleibt auf dem Server.*

Konfigurieren von softwarebasiertem SSL

Bei der Konfiguration von softwarebasiertem SSL können Sie den Anwendungsserver (HTTP), den Meetingserver (RTMP) oder beide sichern. Unabhängig von der gewählten Konfiguration müssen Sie zunächst den DNS-Server konfigurieren.

Konfigurieren Sie den DNS-Server

❖ Erstellen Sie DNS-Einträge, die für jede sichere Verbindung einen FQDN definieren.

Der FQDN für den Anwendungsserver ist die URL, die Endbenutzer zur Verbindung mit Acrobat Connect Pro benutzen. Geben Sie diesen FQDN als Connect Pro Host-Wert auf der Seite „Servereinstellungen“ der Anwendungsverwaltungskonsole ein. Ein geeigneter Wert ist beispielsweise „verbinden“. *meinefirma*.com

Endbenutzer sehen den FQDN für den Meetingserver nicht. Sie müssen allerdings einen FQDN für den Meetingserver haben, wenn Sie Meetings über eine sichere Verbindung veranstalten möchten. Geben Sie diesen FQDN im Feld „Externer Name“ auf der Seite „Servereinstellungen“ der Anwendungsverwaltungskonsole ein. Ein guter Wert ist beispielsweise fms.ihrefirma.com.

Hinweis: *In einem Servercluster können alle Anwendungsserver ein SSL-Zertifikat gemeinsam nutzen, aber jeder Meetingserver muss über ein eigenes Zertifikat verfügen. Auf einem einzelnen Server müssen insgesamt zwei FQDNs und zwei SSL-Zertifikate (für jedes Protokoll eines) vorliegen, um sowohl die HTTP-Verbindung (Anwendungsserver) als auch die RTMP-Verbindung (Meetinserver) abzusichern.*

Meetingserver und den Anwendungsserver sichern.

1 Öffnen Sie die Datei Adaptor.xml im Ordner *[root_install_dir]*\comserv\win32\conf_defaultRoot_ und speichern Sie eine Sicherungskopie in einem anderen Ordner.

2 Fügen Sie den folgenden Code in die Originaldatei Adaptor.xml zwischen die Tags `<Adaptor></Adaptor>` ein (ersetzen Sie den kursiv gedruckten Code durch Ihre eigenen Werten):

```
<SSL>
    <Edge name="meetingserver">
        <SSLServerCtx>
<SSLCertificateFile>[root_install_dir]\sslMeetingPublicCert.pem</SSLCertificateFile>
    <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslMeetingPrivateKey.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
    <Edge name="applicationserver">
        <SSLServerCtx>

<SSLCertificateFile>[root_install_dir]\sslAppServerPublicCert.pem</SSLCertificateFile>
            <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServerPrivateKey.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

Für jede gesicherte Verbindung werden zwei Dateien benötigt: eine Datei für das öffentliche SSL-Zertifikat und eine zweite Datei für den zugehörigen privaten Schlüssel. Der Speicherort für das öffentliche SSL-Zertifikat wird im Tag `<SSLCertificateFile>` festgelegt. Der Speicherort für den privaten Schlüssel wird wird im Tag `<SSLCertificateKeyFile>` festgelegt. Der Server sendet das öffentliche Zertifikat an den Client. Der private Schlüssen verbleibt auf dem Server.

3 Suchen Sie die folgende Zeile in der Datei Adaptor.xml:

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Ersetzen Sie den Code in Schritt 3 durch Folgendes:

```
<HostPort name="meetingserver" ctl_channel=":19350">meetingServerIP:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19351">appServerIP:-443</HostPort>
```

5 Speichern Sie die Datei Adaptor.xml.

6 (Optional) Öffnen Sie die Datei Adaptor.xml in einem Webbrowser, um die Syntax zu validieren.

Wenn der Browser einen Fehler anzeigt, korrigieren Sie ihn und öffnen Sie die Datei erneut im Browser. Wiederholen Sie dies, bis die Datei gültig ist.

7 Öffnen Sie die Datei custom.ini im Stamminstallationsverzeichnis (standardmäßig c:\breeze) und speichern Sie eine Sicherungskopie in einem anderen Ordner.

8 Fügen Sie den folgenden Code in die Datei custom.ini ein, ohne vorhandenen Text zu ersetzen oder zu löschen:

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

Hinweis: *Bei der Datei custom.ini wird zwischen Groß- und Kleinschreibung unterschieden. Nutzen Sie Großbuchstaben für Parameternamen und Kleinbuchstaben für Werte.*

9 Speichern Sie die Datei custom.ini.

10 Öffnen Sie die Datei VHost.xml im Ordner *[root_install_dir]*\comserv\win32\conf_defaultRoot__defaultVHost_ und speichern Sie eine Sicherungskopie in einem anderen Ordner.

11 Suchen Sie die folgende Zeile in der Datei VHost.xml:

```
<RouteEntry></RouteEntry>
```

12 Ersetzen Sie die Zeile in Schritt 11 durch folgenden Code:

```
<RouteEntry protocol="rtmp">*:*;*:${ORIGIN_PORT}</RouteEntry>
```

13 Speichern Sie die Datei VHost.xml.

14 (Optional) Öffnen Sie die Datei VHost.xml in einem Webbrowser, um die Syntax zu validieren.

15 Starten Sie Adobe Connect Pro Server 7 neu:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server stoppen“.

c Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server starten“.

d Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

16 Öffnen Sie die Anwendungsverwaltungskonsole (http://localhost:8510/console oder „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Server 7 konfigurieren“).

17 Wählen Sie im Bildschirm „Anwendungseinstellungen“ die Registerkarte „Servereinstellungen“ und führen Sie die folgenden Schritte aus:

a Geben Sie den FQDN für Ihr Acrobat Connect Pro-Benutzerkonto in das Feld „Connect Pro-Host“ ein. Dieser FQDN ist die URL, die Endbenutzer zur Verbindung mit Acrobat Connect Pro benutzen.

b Geben Sie den FQDN für den Acrobat Connect Pro-Meetingserver in das Feld „Externer Name“ unter „Hostzuordnungen“ ein. Der Server nutzt diesen Wert intern.

Sichern nur des Anwendungsservers

1 Öffnen Sie die Datei Adaptor.xml im Ordner *[root_install_dir]*\comserv\win32\conf_defaultRoot_ und speichern Sie eine Sicherungskopie in einem anderen Ordner.

2 Fügen Sie den folgenden Code in die Originaldatei Adaptor.xml zwischen die Tags `<Adaptor></Adaptor>` ein (ersetzen Sie den kursiv gedruckten Code mit Ihren eigenen Werten):

```
<SSL>
    <Edge name="applicationserver">
        <SSLServerCtx>

<SSLCertificateFile>[root_install_dir]\sslAppServerPublicCert.pem</SSLCertificateFile>
            <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServerPrivateKey.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

Für jede gesicherte Verbindung werden zwei Dateien benötigt: eine Datei für das öffentliche SSL-Zertifikat und eine zweite Datei für den zugehörigen privaten Schlüssel. Der Speicherort für das öffentliche SSL-Zertifikat wird im Tag `<SSLCertificateFile>` festgelegt. Der Speicherort für den privaten Schlüssel wird im Tag `<SSLCertificateKeyFile>` festgelegt. Der Server sendet das öffentliche Zertifikat an den Client. Der private Schlüssen verbleibt auf dem Server.

3 Suchen Sie die folgende Zeile in der Datei Adaptor.xml:

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Fügen Sie den folgenden Code unter der Zeile aus Schritt 3 hinzu:

```
<HostPort name="applicationserver" ctl_channel=":19351">:-443</HostPort>
```

5 Speichern Sie die Datei Adaptor.xml.

6 (Optional) Öffnen Sie die Datei Adaptor.xml in einem Webbrowser, um die Syntax zu validieren.

Wenn der Browser einen Fehler anzeigt, korrigieren Sie ihn und öffnen Sie die Datei erneut im Browser. Wiederholen Sie dies, bis die Datei gültig ist.

7 Öffnen Sie die Datei custom.ini im Stamminstallationsverzeichnis (standardmäßig c:\breeze) und speichern Sie eine Sicherungskopie in einem anderen Ordner.

8 Fügen Sie den folgenden Code in die Datei custom.ini ein, ohne vorhandenen Text zu ersetzen oder zu löschen:

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
```

Hinweis: *Bei der Datei custom.ini wird zwischen Groß- und Kleinschreibung unterschieden. Nutzen Sie Großbuchstaben für Parameternamen und Kleinbuchstaben für Werte.*

9 Speichern Sie die Datei custom.ini.

10 Starten Sie Acrobat Connect Pro Server 7 neu:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server stoppen“.

c Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server starten“.

d Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

Sichern nur des Meetingservers

1 Öffnen Sie die Datei Adaptor.xml im Ordner *[root_install_dir]*\comserv\win32\conf_defaultRoot_ und speichern Sie eine Sicherungskopie in einem anderen Ordner.

2 Fügen Sie den folgenden Code in die Originaldatei Adaptor.xml zwischen die Tags `<Adaptor></Adaptor>` ein (ersetzen Sie den kursiv gedruckten Code mit Ihren eigenen Werten):

```
<SSL>
    <Edge name="meetingserver">
        <SSLServerCtx>

<SSLCertificateFile>[root_install_dir]\sslMeetingServerPublicCert.pem</SSLCertificateFile>
    <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslMeetingServerPrivateKey.pem</SSLCertificateKeyFile>
            <SSLPassPhrase>mypassphrase</SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

Für jede gesicherte Verbindung werden zwei Dateien benötigt: eine Datei für das öffentliche SSL-Zertifikat und eine zweite Datei für den zugehörigen privaten Schlüssel. Der Speicherort für das öffentliche SSL-Zertifikat wird im Tag `<SSLCertificateFile>` festgelegt. Der Speicherort für den privaten Schlüssel wird im Tag `<SSLCertificateKeyFile>` festgelegt. Der Server sendet das öffentliche Zertifikat an den Client. Der private Schlüssen verbleibt auf dem Server.

3 Suchen Sie die folgende Zeile in der Datei Adaptor.xml:

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 Ersetzen Sie den Code in Schritt 3 durch Folgendes:

```
<HostPort name="meetingserver" ctl_channel=":19350">:-443</HostPort>
```

5 Speichern Sie die Datei Adaptor.xml.

6 (Optional) Öffnen Sie die Datei Adaptor.xml in einem Webbrowser, um die Syntax zu validieren.

Wenn der Browser einen Fehler anzeigt, korrigieren Sie ihn und öffnen Sie die Datei erneut im Browser. Wiederholen Sie dies, bis die Datei gültig ist.

7 Öffnen Sie die Datei VHost.xml im Ordner *[root_install_dir]*\comserv\win32\conf_defaultRoot__defaultVHost_ und speichern Sie eine Sicherungskopie in einem anderen Ordner.

8 Suchen Sie die folgende Zeile in der Datei VHost.xml:

```
<RouteEntry></RouteEntry>
```

9 Ersetzen Sie die Zeile in Schritt 8 durch folgenden Code:

```
<RouteEntry protocol="rtmp">*:*;*:${ORIGIN_PORT}</RouteEntry>
```

10 Speichern Sie die Datei VHost.xml.

11 (Optional) Öffnen Sie die Datei VHost.xml in einem Webbrowser, um die Syntax zu validieren.

12 Öffnen Sie die Datei custom.ini im Stamminstallationsverzeichnis (standardmäßig c:\breeze) und speichern Sie eine Sicherungskopie in einem anderen Ordner.

13 Fügen Sie den folgenden Code in die Datei custom.ini ein, ohne vorhandenen Text zu ersetzen oder zu löschen:

```
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

14 Speichern Sie die Datei custom.ini.

15 Starten Sie Acrobat Connect Pro Server 7 neu:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server stoppen“.

c Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server starten“.

d Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

Konfiguration testen

1 Wenn Sie den Anwendungsserver gesichert haben, melden Sie sich bei Connect Pro Central an. Im Browser wird ein Vorhängeschlosssymbol angezeigt.

2 Wenn Sie den Meetingserver gesichert haben, betreten Sie einen Acrobat Connect Pro-Meetingraum. Im Verbindungssymbol wird das Vorhängeschloss angezeigt.

Konfigurieren von hardwarebasiertem SSL

Bei der Konfiguration von hardwarebasiertem SSL können Sie den Anwendungsserver (HTTP), den Meetingserver (RTMP) oder beide sichern. Unabhängig von der gewählten Konfiguration müssen Sie zunächst den DNS-Server konfigurieren.

Weitere Anweisungen zur Konfiguration des Hardwarebeschleunigers können Sie der Dokumentation des Herstellers entnehmen.

DNS-Server konfigurieren

❖ Erstellen Sie DNS-Einträge für alle Server, die Sie sichern möchten.

Definieren Sie für jeden abgesicherten Server eine FQDN (Beispiel: anwendung.beispiel.de und meeting1.bespiel.de).

Hinweis: *In einem Servercluster können alle Anwendungsserver ein SSL-Zertifikat gemeinsam nutzen, aber jeder Meetingserver muss über ein eigenes SSL-Zertifikat verfügen. Auf einem einzelnen Server müssen insgesamt zwei FQDNs und zwei SSL-Zertifikate (für jedes Protokoll eines) vorliegen, um sowohl die HTTP-Verbindung (Anwendungsserver) als auch die RTMP-Verbindung (Meetinserver) abzusichern.*

SSL für die Meeting- und Anwendungsserver konfigurieren

1 Konfigurieren Sie das Hardwaregerät, damit es Folgendes ausführt:

a Port 443 für anwendung.beispiel.com extern überwachen.

b Unverschlüsselte Daten an den Anwendungsserver an Port 8443 weiterleiten.

c Port 443 für meeting1.beispiel.com extern überwachen.

d Unverschlüsselte Daten an den Meetingserver an Port 1935 weiterleiten.

e (Optional) Port 80 für anwendung.beispiel.com extern überwachen und unverschlüsselte Daten an den Anwendungsserver an Port 80 weiterleiten. Der Anwendungsserver leitet Benutzer an Port 443 um.

2 Konfigurieren Sie die Firewall, damit sie Folgendes ausführt:

a Datenverkehr zum Anwendungsserver an Port 443 zulassen (und an Port 80, falls Sie Schritt 1e ausgeführt haben).

b Datenverkehr zum Meetingserver an Port 443 zulassen.

3 Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Server 7 konfigurieren“, um die Anwendungsverwaltungskonsole zu öffnen. Wählen Sie im Bildschirm „Anwendungseinstellungen“ die Registerkarte „Servereinstellungen“ und führen Sie die folgenden Schritte aus:

a Geben Sie den FQDN des Anwendungsservers (z. B. anwendung.beispiel.com) in das Feld „Connect Pro Host“ ein. Dieser FQDN ist die URL, die Endbenutzer zur Verbindung mit Acrobat Connect Pro benutzen.

b Geben Sie den FQDN für den Meetingserver (z. B. fms.beispiel.com) in das Feld „Externer Name“ unter „Hostzuordnungen“ ein. Der Server nutzt diesen Wert intern.

4 Öffnen Sie die Datei custom.ini im Stamminstallationsverzeichnis (standardmäßig c:\breeze) und speichern Sie eine Sicherungskopie in einem anderen Ordner.

5 Fügen Sie den folgenden Code in die Datei custom.ini ein, ohne vorhandenen Text zu ersetzen oder zu löschen:

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

***Hinweis:** Bei der Datei custom.ini wird zwischen Groß- und Kleinschreibung unterschieden. Nutzen Sie Großbuchstaben für Parameternamen und Kleinbuchstaben für Werte.*

6 Speichern Sie die Datei custom.ini.

7 Starten Sie Acrobat Connect Pro Server 7 neu:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

SSL nur für den Meetingserver konfigurieren

1 Konfigurieren Sie das Hardwaregerät, damit es Folgendes ausführt:

a Port 443 für meeting1.beispiel.com extern überwachen.

b Unverschlüsselte Daten an den Meetingserver an Port 1935 weiterleiten.

2 Konfigurieren Sie die Firewall so, dass sie den Datenverkehr zum Meetingserver an Port 443 zulässt.

3 Öffnen Sie die Datei custom.ini im Stamminstallationsverzeichnis (standardmäßig c:\breeze) und speichern Sie eine Sicherungskopie in einem anderen Ordner.

4 Fügen Sie den folgenden Code in die Datei custom.ini ein, ohne vorhandenen Text zu ersetzen oder zu löschen:

```
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

5 Speichern Sie die Datei custom.ini.

SSL nur für den Anwendungsserver konfigurieren

1 Konfigurieren Sie das Hardwaregerät, damit es Folgendes ausführt:

a Port 443 für anwendung.beispiel.com extern überwachen.

b Unverschlüsselte Daten an den Anwendungsserver an Port 8443 weiterleiten.

c (Optional) Port 80 für anwendung.beispiel.com extern überwachen und unverschlüsselte Daten an den Anwendungsserver an Port 80 weiterleiten. Der Anwendungsserver leitet Benutzer an Port 443 um.

2 Konfigurieren Sie die Firewall so, dass sie den Datenverkehr zum Anwendungsserver an Port 443 zulässt (und an Port 80, falls Sie Schritt 1c ausgeführt haben).

3 Fügen Sie der Datei „custom.ini“ im Stamminstallationsordner (standardmäßig c:\breeze) auf Acrobat Connect Pro Folgendes hinzu:

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
```

Hinweis: *Bei der Datei custom.ini wird zwischen Groß- und Kleinschreibung unterschieden. Nutzen Sie Großbuchstaben für Parameternamen und Kleinbuchstaben für Werte.*

4 Starten Sie Acrobat Connect Pro Server 7 neu:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

Testen der Konfiguration

1 Wenn Sie den Anwendungsserver gesichert haben, melden Sie sich bei Connect Pro Central an. Im Browser wird ein Vorhängeschlosssymbol angezeigt.

2 Wenn Sie den Meetingserver gesichert haben, betreten Sie einen Acrobat Connect Pro-Meetingraum. Im Verbindungssymbol wird ein Vorhängeschloss angezeigt.

Konfigurieren von softwarebasiertem SSL für einen Edge-Server

Wenn Sie Software-SSL auf dem Ursprungsserver konfiguriert haben, konfigurieren Sie softwarebasiertes SSL für jeden Edge-Server, den Sie sichern möchten.

Genau wie ein Ursprungsserver leistet ein Edge-Server zwei Dienste: einen Meetingdienst und einen Anwendungsdienst. Um sowohl für den Meeting- als auch den Anwendungsdienst SSL zu konfigurieren, sind zwei FQDNs und zwei IP-Adressen erforderlich. Sie können den FQDN für den Anwendungsdienst mit dem Ursprungsserver teilen, für den Meetingdienst ist aber ein eigener FQDN erforderlich. Der FQDN des Anwendungsdienstes ist die URL, die Benutzer nutzen, um eine Verbindung mit Ihren Acrobat Connect Pro-Benutzerkonten herzustellen.

Wenn Sie beispielsweise einen Edge-Server und einen Ursprungsserver haben, benötigen Sie drei FDQNs und drei SSL-Zertifikate: für jeden Meetingdienst und für die gemeinsamen Anwendungsdienste. Außerdem sind vier IP-Adressen erforderlich, eine für jeden Meetingdienst und eine für jeden Anwendungsdienst.

In diesem Beispiel hat der Ursprungsserver die folgenden IP-Adressen und FQDNs:

```
10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com
```

Der Edge-Server hat die folgenden IP-Adressen und FQDNs:

```
10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com
```

Hinweis: *Wenn Sie sowohl den Edge- als auch den Ursprungsserver erstmalig installieren, richten Sie beide Server ohne SSL ein und stellen Sie sicher, dass die beiden miteinander kommunizieren können. Sobald Sie sicher sind, dass Edge- und Ursprungsserver kommunikationsbereit sind, können Sie für beide Server SSL konfigurieren.*

Verwandte Themen

„Bereitstellen von Acrobat Connect Pro Edge Server“ auf Seite 29

„Informationen zur SSL-Unterstützung“ auf Seite 68

Edge-Server konfigurieren

1 Öffnen Sie auf dem Ursprungsserver die Datei c:\breeze\comserv\win32\conf_defaultRoot_\Adaptor.xml und kopieren Sie den gesamten Abschnitt `<SSL></SSL>` wie folgt:

```
<SSL>
    <Edge name="applicationserver">
        <SSLServerCtx>
        <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
            <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.comKEY.pem
            </SSLCertificateKeyFile>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
    <Edge name="meetingserver">
        <SSLServerCtx>
            <SSLCertificateFile>C:\breeze\meetingPublicCert.pem
            </SSLCertificateFile>
            <SSLCertificateKeyFile type="PEM">C:\breeze\meetingPrivateKey.pem
            </SSLCertificateKeyFile>
            <SSLPassPhrase></SSLPassPhrase>
            <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
            <SSLSessionTimeout>5</SSLSessionTimeout>
        </SSLServerCtx>
    </Edge>
</SSL>
```

Hinweis: *Ihr Code kann unterschiedliche Werte beinhalten, aber er muss dieselben XML-Elemente aufweisen.*

2 Öffnen Sie auf dem Edge-Server die Datei c:\breeze\edgeserver\win32\conf_defaultRoot_\Adaptor.xml und kopieren Sie den Codeblock `<SSL></SSL>` vom Ursprungsserver an die Stelle nach dem Tag `<Adaptor>` .

3 Gehen Sie wie folgt vor, um den Anwendungsdienst und den Meetingdienst auf dem Edge-Server zu konfigurieren:

a Der Anwendungsdienst ist das Tag `<Edge name="applicationserver">` innerhalb des `<SSL>` -Blocks. Der Anwendungsdienst nutzt denselben FQDN wie der Anwendungsdienst auf dem Ursprungsserver. Kopieren Sie die Zertifikat- und wichtige.pem-Dateien vom Ursprungsserver an denselben Ort auf dem Edge-Server. In diesem Beispiel lautet der FQDN connect.ihrefirma.com.

```
<Edge name="applicationserver">
    <SSLServerCtx>
        <SSLCertificateFile>C:\breeze\connect.yourcompany.com.pem</SSLCertificateFile>
        <SSLCertificateKeyFile type="PEM">C:\breeze\connect.yourcompany.comKEY.pem
            </SSLCertificateKeyFile>
        <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
        <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
</Edge>
```

b Der Meetingdienst ist das Tag `<Edge name="meetingserver">` innerhalb des `<SSL>` -Blocks. Bearbeiten Sie die XML-Datei, sodass der Meetingdienst auf ein eindeutiges Zertifikat und einen Schlüssel für seinen eindeutigen FQDN verweist. In diesem Beispiel lautet der FQDN edge1.ihrefirma.com:

```
<Edge name="meetingserver">
    <SSLServerCtx>
        <SSLCertificateFile>C:\breeze\edge1.yourcompany.com.pem
        </SSLCertificateFile>
        <SSLCertificateKeyFile type="PEM">C:\breeze\edge1.yourcompany.comKEY.pem
        </SSLCertificateKeyFile>
        <SSLPassPhrase></SSLPassPhrase>
        <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
        <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
</Edge>
```

4 Suchen Sie in der Datei Adaptor.xml auf dem Edge-Server nach der Zeile `<HostPort name="edge1">${FCS.HOST_PORT}</HostPort>`. Fügen Sie nach dieser Zeile die folgenden zwei Zeilen ein:

```
<HostPort name="meetingserver" ctl_channel=":19354">206.192.37.100:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19355">206.192.37.101:-443</HostPort>
```

Dieser Code bindet die internen IP-Adressen des Edge-Servers an den sicheren Port 443. In diesem Beispiel werden die internen IP-Adressen 206.192.37.100 und 206.192.37.101 verwendet. Ersetzen Sie in Ihrem Code die internen IP-Adressen Ihres Edge-Servers.

5 Speichern Sie die Datei Adaptor.xml.

6 Öffnen Sie die Datei Adaptor.xml in einem Webbrowser, um sicherzustellen, dass sie gültig ist.

Falls Syntaxfehler vorhanden sind, zeigt der Webbrowser eine Fehlermeldung an. Korrigieren Sie die XML-Fehler und überprüfen Sie die Datei erneut.

7 Öffnen Sie auf dem Edge-Server die Datei c:\breeze\edgeserver\win32\conf_defaultRoot__defaultVHost_\Vhost.xml. Suchen Sie nach dem Tag `<RouteEntry></RouteEntry>` und ersetzen Sie es folgendermaßen:

```
<RouteEntry protocol="rtmp">*:*;10.192.37.11:8506</RouteEntry>
```

Dieser Code hat zur Folge, dass der Edge-Server RTMP-Verbindungen von jeder beliebigen IP-Adresse und jedem Port über Port 8506 an den Ursprungsserver routet. In diesem Beispiel wird die IP-Adresse 10.192.37.11 verwendet. Ersetzen Sie in Ihrem Code die IP-Adresse des Anwendungsdienstes auf dem Ursprungsserver.

8 Speichern Sie die Datei VHost.xml.

9 Öffnen Sie die Datei Vhost.xml in einem Webbrowser, um sicherzustellen, dass sie gültig ist.

Falls Syntaxfehler vorhanden sind, zeigt der Webbrowser eine Fehlermeldung an. Korrigieren Sie die XML-Fehler und überprüfen Sie die Datei erneut.

10 Öffnen Sie auf dem Edge-Server die Datei „c:\breeze\edgeserver\custom.ini file“.

11 Geben Sie den Parameter `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` ein und stellen Sie ihn wie folgt entweder auf die IP-Adresse oder den FQDN des Ursprungsservers ein:

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

Wenn Sie Ihr System so konfigurieren möchten, dass eine Verbindung ausschließlich über SSL hergestellt wird, formulieren Sie den Parameter `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` wie folgt aus:

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

Hinweis: *Wenn der Edge-Server Schwierigkeiten hat, den FQDN des Ursprungsservers aufzulösen, nutzen Sie die IP-Adresse.*

12 Öffnen Sie auf dem Edge-Server die Datei C:\breeze\edgeserver\win32\conf\HttpCache.xml und aktualisieren Sie das Tag `<HostName>` wie folgt:

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

13 Speichern Sie die Datei HttpCache.xml.

14 Öffnen Sie die Datei HttpCache.xml in einem Webbrowser, um sicherzustellen, dass sie gültig ist.

Falls Syntaxfehler vorhanden sind, zeigt der Webbrowser eine Fehlermeldung an. Korrigieren Sie die XML-Fehler und versuchen Sie es erneut.

Konfigurieren Sie den Ursprungsserver

1 Konfigurieren Sie den Ursprungsserver für SSL. Weitere Informationen finden Sie unter „SSL (Secure Sockets Layer)“ auf Seite 68.

2 Öffnen Sie auf dem Ursprungsserver die Datei c:\breeze\custom.ini und geben Sie Folgendes ein, um den Edge-Server an den Ursprungsserver zu binden:

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Verwenden Sie den für den Parameter in der Datei „custom.ini“ `FCS_EDGE_CLUSTER_ID` eingestellten Wert auf dem Edge-Server. In diesem Beispiel lautet der Wert `sanfran`, der Code ist `edge.sanfran=1`.

Hinweis: *Der Wert 0 ist vorbehalten und kann nicht verwendet werden.*

3 Starten Sie Connect Pro Central Application Server und Connect Pro Meeting Server erneut.

4 Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Server 7 konfigurieren“, um die Anwendungsverwaltungskonsole zu öffnen. Führen Sie folgende Schritte aus:

a Klicken Sie auf „Servereinstellungen“.

b Im Feld „Externe Namen“ sehen Sie den FQDN des Edge-Servers und rechts daneben ein leeres Kästchen. Wenn Sie den FQDN nicht sehen, warten Sie einige Minuten und aktualisieren Sie den Browser.

c Geben Sie den FQDN des Edge-Servers im leeren Kästchen ein und klicken Sie auf „Speichern“. Der Edge-Server ist nun mit beim Ursprungsserver registriert.

5 Richten Sie den lokalen DNS-Server ein, um Benutzer, die eine Acrobat Connect Pro-URL anfordern, an den Edge-Server weiterzuleiten.

Konfigurieren von hardwarebasiertem SSL für einen Edge-Server

Wenn Sie Hardware-SSL auf dem Ursprungsserver konfiguriert haben, konfigurieren Sie hardwarebasiertes SSL für jeden Edge-Server, den Sie sichern möchten.

Genau wie ein Ursprungsserver leistet ein Edge-Server zwei Dienste: einen Meetingdienst und einen Anwendungsdienst. Um sowohl für den Meeting- als auch den Anwendungsdienst SSL zu konfigurieren, sind zwei FQDNs und zwei IP-Adressen erforderlich. Sie können den FQDN für den Anwendungsdienst mit dem Ursprungsserver teilen, für den Meetingdienst ist aber ein eigener FQDN erforderlich. Der FQDN des Anwendungsdienstes ist die URL, die Benutzer nutzen, um eine Verbindung mit Ihren Acrobat Connect Pro-Benutzerkonten herzustellen.

Wenn Sie beispielsweise einen Edge-Server und einen Ursprungsserver haben, benötigen Sie drei FDQNs und drei SSL-Zertifikate: für jeden Meetingdienst und für die gemeinsamen Anwendungsdienste. Außerdem sind vier IP-Adressen erforderlich, eine für jeden Meetingdienst und eine für jeden Anwendungsdienst.

In diesem Beispiel hat der Ursprungsserver die folgenden IP-Adressen und FQDNs:

```
10.192.37.11 = connect.yourcompany.com
10.192.37.10 = meeting1.yourcompany.com
```

Der Edge-Server hat die folgenden IP-Adressen und FQDNs:

```
10.192.37.100 = connect.yourcompany.com
10.192.37.101 = edge1.yourcompany.com
```

Hinweis: *Wenn Sie sowohl den Edge- als auch den Ursprungsserver erstmalig installieren, richten Sie beide Server ohne SSL ein und stellen Sie sicher, dass die beiden miteinander kommunizieren können. Sobald Sie sichergestellt haben, dass Edge- und Ursprungsserver kommunikationsbereit sind, können Sie für beide Server SSL konfigurieren.*

Verwandte Themen

„Bereitstellen von Acrobat Connect Pro Edge Server“ auf Seite 29

„Informationen zur SSL-Unterstützung“ auf Seite 68

Edge-Server konfigurieren

1 Öffnen Sie auf dem Edge-Server die Datei „c:\breeze\edgeserver\custom.ini file“.

2 Geben Sie den Parameter `FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT` ein und stellen Sie ihn wie folgt entweder auf die IP-Adresse oder den FQDN des Ursprungsservers ein:

```
FCS.HTTPCACHE_BREEZE_SERVER_SECURE_PORT=connect.yourcompany.com:443
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
FCS_EDGE_HOST=edge1.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=sanfran
FCS_EDGE_EXPIRY_TIME=60000
FCS_EDGE_REG_INTERVAL=30000
```

Wenn Sie Ihr System so konfigurieren möchten, dass eine Verbindung ausschließlich über SSL hergestellt wird, formulieren Sie den Parameter `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT` wie folgt aus:

```
# FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

Hinweis: *Wenn der Edge-Server Schwierigkeiten hat, den FQDN des Ursprungsservers aufzulösen, nutzen Sie die IP-Adresse.*

3 Öffnen Sie auf dem Edge-Server die Datei C:\breeze\edgeserver\win32\conf\HttpCache.xml und aktualisieren Sie das Tag `<HostName>` wie folgt:

```
<HostName>${FCS_EDGE_HOST}</HostName>
```

4 Speichern Sie die Datei HttpCache.xml.

5 Öffnen Sie die Datei HttpCache.xml in einem Webbrowser, um sicherzustellen, dass sie gültig ist.

Falls Syntaxfehler vorhanden sind, zeigt der Webbrowser eine Fehlermeldung an. Korrigieren Sie die XML-Fehler und versuchen Sie es erneut.

Konfigurieren Sie den Ursprungsserver

1 Konfigurieren Sie den Ursprungsserver für SSL. Weitere Informationen finden Sie unter „SSL (Secure Sockets Layer)“ auf Seite 68.

2 Öffnen Sie auf dem Ursprungsserver die Datei c:\breeze\custom.ini und geben Sie Folgendes ein, um den Edge-Server an den Ursprungsserver zu binden:

```
edge.FCS_EDGE_CLUSTER_ID=1
```

Verwenden Sie den für den Parameter in der Datei „custom.ini“ `FCS_EDGE_CLUSTER_ID` eingestellten Wert auf dem Edge-Server. In diesem Beispiel lautet der Wert `sanfran`, der Code ist `edge.sanfran=1`.

Hinweis: *Der Wert 0 ist vorbehalten und kann nicht verwendet werden.*

3 Starten Sie Connect Pro Central Application Server und Connect Pro Meeting Server erneut.

4 Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Server 7 konfigurieren“, um die Anwendungsverwaltungskonsole zu öffnen. Führen Sie folgende Schritte aus:

a Klicken Sie auf „Servereinstellungen“.

b Im Feld „Externe Namen“ sehen Sie den FQDN des Edge-Servers und rechts daneben ein leeres Kästchen. Wenn Sie den FQDN nicht sehen, warten Sie einige Minuten und aktualisieren Sie den Browser.

c Geben Sie den FQDN des Edge-Servers im leeren Kästchen ein und klicken Sie auf „Speichern“. Der Edge-Server ist nun mit beim Ursprungsserver registriert.

5 Richten Sie den lokalen DNS-Server ein, um Benutzer, die eine Acrobat Connect Pro-URL anfordern, an den Edge-Server weiterzuleiten.

SSL XML-Tags

Tag	Standardwert	Beschreibung
`SSLCertificateFile`	Kein Standardwert	Der Speicherort der Zertifizierungsdatei, die an den Client gesendet werden soll. Sofern Sie keinen absoluten Pfad angeben, wird davon ausgegangen, dass die Position des Zertifikats relativ zum Verzeichnis „Adaptor“ angegeben ist.
`SSLCertificateKeyFile`	Kein Standardwert	Der Speicherort der Datei mit dem privaten Schlüssel für das Zertifikat. Sofern Sie keinen absoluten Pfad angeben, wird davon ausgegangen, dass die Position der Schlüsseldatei relativ zum Verzeichnis „Adaptor“ angegeben ist. Handelt es sich um eine verschlüsselte Datei, muss das Kennwort im Tag `SSLPassPhrase` angegeben sein. Das Attribut `type` gibt den Typ der für die Zertifikatsschlüsseldatei verwendeten Codierung an. Typen können entweder `PEM` oder `ASN1` sein.

Tag	Standardwert	Beschreibung
`SSLCipherSuite`	Siehe Beschreibung	Der Verschlüsselungsalgorithmus. Der Algorithmus besteht aus durch Doppelpunkte getrennten Elementen. Bei diesen Elementen kann es sich um Algorithmen zum Austauschen von Schlüsseln, um Authentifizierungs- oder Verschlüsselungsverfahren, um Digest-Typen oder um einen Alias-Namen für gebräuchliche Gruppierungen handeln. Eine Aufstellung aller Komponenten finden Sie in der Flash Media Server-Dokumentation. Für dieses Tag gilt die folgende Standardeinstellung: `ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH` Ändern Sie die Standardeinstellungen nur nach vorheriger Rücksprache mit dem technischen Support von Adobe.
`SSLPassPhrase`	Kein Standardwert	Das Kennwort für die Entschlüsselung der Datei mit dem privaten Schlüssel. Falls die Datei mit dem privaten Schlüssel nicht verschlüsselt ist, lassen Sie dieses Tag leer.
`SSLSessionTimeout`	5	Die Gültigkeitsdauer einer SSL-aktivierten Sitzung in Minuten.

SSL-Konfigurationsparameter

Parameter	Standardwert	Beschreibung
`ADMIN_PROTOCOL`	`http://`	Das vom Anwendungsserver verwendete Protokoll. Verwenden Sie `https://` für die SSL-Konfiguration.
`DEFAULT_FCS_HOSTPORT`	`:1935`	Der Port, der von Flash Media Server für die Kommunikation via RTMP verwendet wird. Verwenden Sie 443,1935 für die SSL-Konfiguration.
`HTTPS_PORT`	Kein Standardwert.	Der Port, den der Anwendungsserver für HTTPS-Anfragen überwacht. Dieser Parameter ist bei der SSL-Konfiguration normalerweise auf `443` oder `8443` eingestellt.
`SSL_ONLY`	`no`	Verwenden Sie `yes`, wenn der Server nur sichere Verbindungen unterstützt. Diese Einstellung zwingt alle Acrobat Connect Pro-URLs, HTTPS zu verwenden.
`RTMP_SEQUENCE`	Kein Standardwert.	Die Ursprungsserver, Egde-Server und Ports, die für die Verbindung zu Flash Media Server (dem Meetingserver) verwendet werden.

PKI (Public Key-Infrastruktur)

Informationen zu PKI (Public Key-Infrastruktur)

Sie können eine Public-Key-Infrastruktur (PKI) einrichten, um Anmeldedaten als Teil der Sicherheitsarchitektur von Acrobat Connect Pro für Clients zu verwalten. Im bekannteren SSL-Protokoll muss sich der Server gegenüber dem Client identifizieren; in einer PKI muss sich der Client gegenüber dem Server identifizieren.

Ein vertrauenswürdiger Drittanbieter, die so genannte Zertifizierungsstelle, bestätigt die Identität eines Clients und bindet ein Zertifikat an diesen Client. Das Zertifikat (auch als *Public Key* bekannt) wird im X.509-Format ausgestellt. Wenn ein Client eine Verbindung zu Acrobat Connect Pro herstellt, wickelt ein Proxy die Verbindung für die PKI ab. Falls der Client über einen Cookie aus einer früheren Sitzung oder über ein gültiges Zertifikat verfügt, wird der Client mit Acrobat Connect Pro verbunden.

Weitere Informationen zur PKI erhalten Sie im Microsoft PKI Technology Center.

PKI-Benutzeranforderungen

Benutzer müssen Windows XP oder Windows 2003 verwenden, und auf ihren lokalen Computern muss ein gültiges Client-Zertifikat installiert sein, um an einem Meeting mit PKI-Authentifizierung teilnehmen zu können. Wenn ein Benutzer an einem Meeting teilnimmt, wird ihm ein Dialogfeld angezeigt, in dem er unter den Zertifikaten, die auf seinem Computer installiert sind, ein gültiges Client-Zertifikat auswählen kann.

Es wird empfohlen, dass Clients das Adobe Acrobat Connect-Add-In verwenden, um an Meetings teilzunehmen, für die eine PKI-Authentifizierung erforderlich ist. Clients müssen das Add-In mithilfe des eigenständigen Installationsprogramms für das Add-In installieren, bevor sie an einem Meeting teilnehmen.

Clients können auch die neueste Version von Adobe Flash Player im Browser verwenden, um an Meetings teilzunehmen, die PKI-Unterstützung von Flash Player ist allerdings nicht so weitreichend wie die des Add-Ins. Für die Anzeige von archivierten Meetings müssen Clients über die neueste Version des Flash Players verfügen.

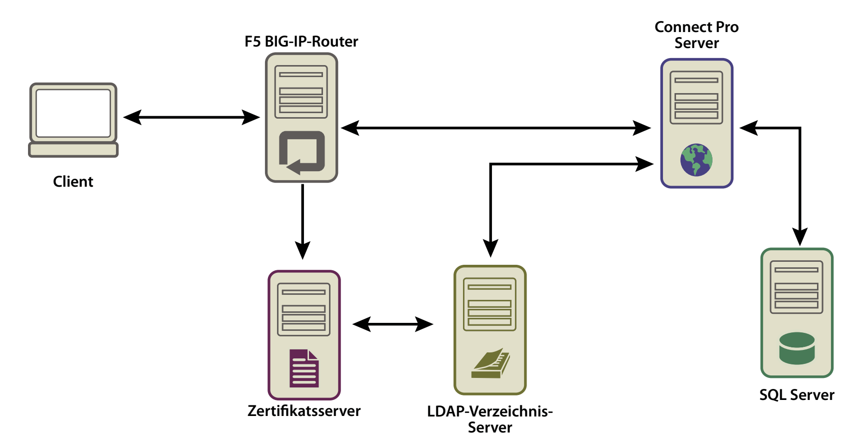
Sie können ein PKI-System entwerfen, um die Authentifizierung nur für HTTP-Verbindungen oder für HTTP- und RTMP-Verbindungen zu verlangen. Wenn Sie für HTTP- und RTMP-Verbindungen clientseitige Zertifikate verlangen, werden Benutzer jedes Mal, wenn eine neue Serververbindung hergestellt wird, zur Eingabe aufgefordert. Für die Anmeldung bei einem Meeting gibt es dann zwei Eingabeaufforderungen, eine für HTTP und eine für RTMP. Eine RTMP-Verbindung kann nicht ohne HTTP-Authentifizierung hergestellt werden, deshalb können Sie die clientseitige Authentifizierung ggf. auch nur für die HTTP-Verbindung verlangen.

Implementieren von PKI

Nachstehend wird als Beispiel Schritt für Schritt die Implementierung einer PKI mit einem F5 BIG-IP LTM 9.1.2 (Build 40.2)-Router als Proxy beschrieben. Verwenden Sie die relevanten Abschnitte, um Ihre eigene Lösung zu erstellen (mit einem F5-Router oder einem anderen Gerät).

In dieser Beispielimplementierung werden strikte Sicherheitsstandards eingehalten; so ist z. B. die clientseitige Zertifizierung für HTTP-Verbindungen (Anwendungsserver) und RTMP-Verbindungen (Meetingserver) erforderlich.

Hinweis: *Es wird dringend empfohlen, vor der PKI-Implementierung Sicherheitsrichtlinien zu erstellen. In der PKI können viele unterschiedliche Technologien zum Einsatz kommen; deshalb ist die Gewährleistung der Sicherheit wichtig, wenn diese Systeme interagieren.*



Datenfluss in einer Public-Key-Infrastruktur

In diesem Beispiel wird Folgendes vorausgesetzt:

- Acrobat Connect Pro ist installiert.

- Acrobat Connect Pro ist mit einem LDAP-Verzeichnisdienst integriert.
- Ein aus dem LDAP-Verzeichnisdienst importierter Benutzer kann an einem von Acrobat Connect Pro bereitgestellten Meeting teilnehmen.
- Ein F5-Router ist installiert.

1. Konfigurieren Sie den LDAP-Verzeichnisserver

Für jeden Benutzer muss ein LDAP-`E-Mail`-Attribut festgelegt werden. Dieses Attribut wird dem Betrefffeld des Client-Zertifikats hinzugefügt.

Die F5 iRule analysiert das X.509::subject, um die E-Mail-Adresse zu finden, und fügt den Wert in den HTTP-Header ein Acrobat Connect Pro nutzt den HTTP-Header zur Benutzerauthentifizierung.

Hinweis: *In diesem Beispiel wird das Attribut* `E-Mail` *verwendet. Sie können eine beliebige eindeutige Kennung verwenden, die das Format X.509 unterstützt, höchstens 254 Zeichen enthält und vom LDAP-Verzeichnisdienst und Acrobat Connect Pro gemeinsam verwendet wird.*

2. Legen Sie die Anmelderichtlinien für Acrobat Connect Pro fest.

Acrobat Connect Pro muss eine E-Mail-Adresse für die Benutzeranmeldung verwenden. Wählen Sie in Connect Pro Central die Registerkarte „Administration“, klicken Sie auf „Benutzer und Gruppen“ und dann auf „Anmelde- und Kennwortrichtlinien bearbeiten“.

3. Konfigurieren Sie einen CA-Server.

Die Zertifizierungsstelle (Certification Authority, CA) verarbeitet Zertifizierunganfragen, überprüft Client-Identitäten, gibt Zertifikate aus und verwaltet eine Liste mit widerrufenen Zertifikaten (Client Revocation List, CRL).

In dieser Implementierung weist die CA auf den LDAP-Verzeichnisserver, um ein Client-Zertifikat zu erhalten. Die Zertifizierungsstelle fragt den LDAP-Server nach den Client-Informationen. Wenn diese vorhanden sind und nicht widerrufen wurden, werden sie in ein Zertifikat formatiert.

Überprüfen Sie, ob das Client-Zertifikat installiert wurde und verwendet werden kann, indem Sie sich das Betrefffeld ansehen. Es sieht wie folgt aus:

```
E = adavis@asp.sflab.macromedia.com
CN = Andrew Davis
CN = Users
DC = asp
DC = sflab
DC = macromedia
DC = com
```

4. Konfigurieren Sie Acrobat Connect Pro für die Verwendung der HTTP-Header-Authentifizierung.

Entfernen Sie in der Datei „*[Stamm-Installationsverzeichnis]*\appserv\conf\WEB-INF\web.xml“ die Kommentarmarkierung von den folgenden Codezeilen:

```
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

Meetingserver und den Anwendungsserver beenden. Fügen Sie der Datei „custom.ini“ im Stamm-Installationsverzeichnis die folgende Zeile hinzu:

```
HTTP_AUTH_HEADER=hah_login
```

Speichern Sie die Datei „custom.ini“ und starten Sie Acrobat Connect Pro neu.

5. Konfigurieren Sie die F5-Anwendungslogik.

Die Anwendungslogik in F5 analysiert das Betrefffeld des Client-Zertifikats, um die E-Mail-Adresse zu finden. Die Logik übergibt die E-Mail-Adresse dann in einem zusätzlichen HTTP-Header an Acrobat Connect Pro.

Ein Client ohne Zertifikat wird abgelehnt. Wenn der Client über ein Zertifikat verfügt, muss es authentifiziert werden. Beispiele für Authentifizierungsmechanismen sind OCSP (Online Certification Status Protocol) und das Nachschlagen über LDAP.

Nach der Authentifizierung des Zertifikats wird es nach einer eindeutigen, Acrobat Connect Pro bekannten Kennung durchsucht. In diesem Beispiel wird ein gültiges Zertifikat nach einer E-Mail-Adresse durchsucht.

Eine Anfrage mit der Zeichenfolge `session` oder dem Cookie `BREEZESESSION` wird ohne weitere Authentifizierung zugelassen, da der Client bereits authentifiziert wurde. (Acrobat Connect Pro überprüft diese Argumente mithilfe einer Datenbankabfrage.)

Ist die Zeichenfolge `session` bzw. der Cookie `BREEZESESSION` nicht in der Anfrage enthalten, muss sich der Benutzer zum Verbinden mit Acrobat Connect Pro anmelden. Zum Anmelden eines Benutzers wird die eindeutige Kennung (hier die E-Mail-Adresse) in das Feld `HTTP_AUTH_HEADER` eingegeben. Die Anfrage wird an die Anmeldeseite von Acrobat Connect Pro geleitet.

Bei dem folgenden Code handelt es sich um eine F5 iRule im HTTPS-Profil, das Anforderungen verarbeitet:

```
set id [SSL::sessionid]
set the_cert [session lookup ssl $id]
set uname [X509::subject $the_cert]
set emailAddr [getfield $uname "emailAddress=" 2]
if { [HTTP::cookie exists BREEZESESSION] } {
    set cookie_payload [HTTP::cookie value BREEZESESSION]
}
elseif { [HTTP::uri] contains "/system/login" }
{
    # Connection has been redirected to the "login page"
    # The email address has been parsed from the certificate
    #
    HTTP::header insert hah_login $emailAddr
}
elseif { [HTTP::uri] contains "session" }
{
    #do nothing, Acrobat Connect Pro verifies the token found in session=$token
}
else
{
    # URI encode the current request, and pass it to
    # the Acrobat Connect Pro system login page because the client
    # does not have a session yet.
    HTTP::redirect https://[HTTP::host]/system/login/ok?next=[URI::encode
https://[HTTP::host][HTTP::uri]]
}
```

Verwandte Themen

„Starten und Beenden von Acrobat Connect Pro Server“ auf Seite 91

Sichern der Infrastruktur

Netzwerksicherheit

Das Kommunikationsmodell von Acrobat Connect Pro stützt sich auf mehrere private TCP/IP-Dienste. Diese Dienste öffnen verschiedene Ports und Kanäle, die vor Benutzern von außerhalb geschützt werden müssen. Für Acrobat Connect Pro ist es erforderlich, dass Sie wichtige Ports durch eine Firewall abschirmen. Die Firewall sollte SPI (Stateful Packet Inspection) unterstützen, nicht nur das Packet-Filtering. Die Firewall sollte über eine Option verfügen, mit der standardmäßig alle Dienste außer den ausdrücklich erlaubten abgelehnt werden. Die Firewall sollte mindestens eine Dual-Home-Firewall sein (also mindestens zwei Netzwerkschnittstellen haben). Diese Architektur trägt dazu bei, dass nicht autorisierte Benutzer die Sicherheit der Firewall nicht umgehen können.

Die einfachste Lösung zur Sicherung von Acrobat Connect Pro besteht darin, alle Ports auf dem Server außer Port 80, Port 1935 sowie Port 443 zu blockieren. Eine externe Hardware-Firewall bietet Schutz vor Sicherheitslücken im Betriebssystem. Sie können mehrere Schichten von Hardware-Firewalls konfigurieren, die so genannte demilitarisierte Zonen (DMZs) bilden. Wenn der Server von Ihrer IT-Abteilung sorgfältig mit den aktuellen Sicherheits-Patches von Microsoft aktualisiert wird, kann eine Software-Firewall konfiguriert werden, um die Sicherheit noch weiter zu erhöhen.

Intranetzugriff

Wenn der Zugriff auf Acrobat Connect Pro über Ihr Intranet erfolgen soll, erstellen Sie für Ihre Acrobat Connect Pro-Server und Ihre Acrobat Connect Pro-Datenbank ein separates Subnetzwerk und schirmen Sie dieses mit einer Firewall ab. Das interne Netzwerksegment, in dem Acrobat Connect Pro installiert wird, sollte private IP-Adressen verwenden (10.0.0.0/8, 172.16.0.0/12 oder 192.168.0.0/16), um es Angreifern zu erschweren, Netzwerkverkehr zu einer öffentlichen IP-Adresse bzw. von der übersetzten internen IP-Adresse zu leiten. Weitere Informationen finden Sie unter RFC 1918. Bei der Konfiguration der Firewall sollten alle Acrobat Connect Pro-Ports berücksichtigt werden sowie die Konfiguration dieser Ports für den eingehenden oder ausgehenden Datenverkehr.

Datenbankserver-Sicherheit

Unabhängig davon, ob Sie Ihre Datenbank auf demselben Server wie Acrobat Connect Pro hosten oder nicht, müssen Sie für die Sicherheit Ihrer Datenbank Sorge tragen. Computer, auf denen eine Datenbank gehostet wird, sollten an einem sicheren Ort aufgestellt werden. Im Folgenden werden weitere Vorsichtsmaßnahmen aufgelistet:

- Installieren Sie die Datenbank in der sicheren Zone Ihres Intranets.
- Die Datenbank darf nie direkt an das Internet angeschlossen werden.
- Legen Sie in regelmäßigen Abständen von allen Daten Sicherungskopien an und bewahren Sie die Kopien an einem sicheren, externen Lagerort auf.
- Installieren Sie die neuesten Patches für Ihren Datenbankserver.
- Verwenden Sie geschützte SQL-Verbindungen.

Informationen zur Sicherung von SQL Server finden Sie auf der Sicherheitswebsite für Microsoft SQL.

Erstellen von Dienstkonten

Acrobat Connect Pro wird sicherer ausgeführt, wenn Sie ein Dienstkonto für Acrobat Connect Pro erstellen. Adobe empfiehlt das Erstellen eines Servicekontos und eines Kontos für SQL Server 2005 Express Edition für Acrobat Connect Pro. Weitere Informationen finden Sie in den Microsoft-Artikeln „How to change the SQL Server or SQL Server Agent service account without using SQL Enterprise Manager in SQL Server 2000 or SQL Server Configuration Manager in SQL Server 2005“ und „The Services and Service Accounts Security and Planning Guide“.

Erstellen eines Dienstkontos

1 Erstellen Sie ein lokales Konto mit dem Namen ConnectService, das keine Standardgruppen enthält.

2 Legen Sie die Dienste Adobe Connect Enterprise, Flash Media Administration Server und Flash Media Server (FMS) für dieses neue Konto fest.

3 Legen Sie den Vollzugriff für den folgenden Registrierungsschlüssel fest:

```
HKLM\SYSTEM\ControlSet001\Control\MediaProperties\PrivateProperties\Joystick\Winmm
```

4 Legen Sie den Vollzugriff in den NTFS-Ordnern im Stammverzeichnis von Acrobat Connect Pro (standardmäßig c:\breeze) fest.

Für Unterordner und Dateien müssen dieselben Berechtigungen gelten. Für Cluster modifizieren Sie die entsprechenden Pfade auf jedem Computerknoten.

5 Legen Sie die folgenden Anmeldeberechtigungen für das ConnectService-Konto fest:

Als Dienst anmelden – SeServiceLogonRight

Erstellen eines Servicekontos für SQL Server 2005 Express Edition

1 Erstellen Sie ein lokales Konto mit dem Namen ConnectSqlService, das keine Standardgruppen enthält.

2 Ändern Sie das Servicekonto für SQL Server 2005 Express Edition von LocalSystem auf ConnectSQLService.

3 Legen Sie den Vollzugriff für ConnectSqlService für die folgenden Registrierungsschlüssel fest:

```
HKEY_LOCAL_MACHINE\Software\Clients\Mail
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\80
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\[databaseInstanceName]
```

Bei Clustern führen Sie diesen Schritt für alle Knoten im Cluster aus. Die Berechtigung „Vollzugriff“ gilt für alle untergeordneten Schlüssel einer benannten Datenbankinstanz.

4 Legen Sie den Vollzugriff für ConnectSqlService in den Datenbankordnern fest. Für Unterordner und Dateien müssen dieselben Berechtigungen gelten. Für Cluster modifizieren Sie die entsprechenden Pfade auf jedem Computerknoten.

5 Legen Sie die folgenden Benutzerrechte für den ConnectSqlService-Dienst fest:

Einsetzen als Teils des Betriebssystems—SeTcbPrivilege Auslassen der durchsuchenden Prüfung—SeChangeNotify Seiten im Speicher sperren—SeLockMemory Anmelden als Stapelverarbeitungsauftrag—SeBatchLogonRight Als Dienst anmelden—SeServiceLogonRight Ersetzen eines Prozessebenentokens—SeAssignPrimaryTokenPrivilege

Sichern von Installationen auf einem einzelnen Server

Der folgende Arbeitsablauf fasst den Prozess der Einrichtung und Absicherung von Acrobat Connect Pro auf einem einzelnen Computer zusammen. Dabei wird davon ausgegangen, dass die Datenbank auf demselben Computer installiert wird und dass Benutzer über das Internet auf Acrobat Connect Pro zugreifen.

1. Installieren Sie eine Firewall.

Da die Benutzer über das Internet auf Acrobat Connect Pro zugreifen können, ist der Server potenziellen Angriffen durch Hacker ausgeliefert. Mit einer Firewall können Sie den Zugriff auf den Server blockieren und gleichzeitig steuern, welche Art von Kommunikation zwischen dem Internet und dem Server zulässig ist.

2. Konfigurieren Sie die Firewall.

Nach der Installation konfigurieren Sie die Firewall wie nachstehend beschrieben:

- Inbound-Ports (vom Internet): 80, 443, 1935.
- Outbound-Ports (zum Mailserver): 25.
- Ausschließliche Verwendung des TCP/IP-Protokolls.

  Da die Datenbank sich auf demselben Server wie Acrobat Connect Pro befindet, müssen Sie Port 1434 auf der Firewall nicht öffnen.

3. Installieren Sie Acrobat Connect Pro

4. Überprüfen Sie die korrekte Funktionsweise der Acrobat Connect Pro-Anwendungen.

Nachdem Sie Acrobat Connect Pro installiert haben, überzeugen Sie sich sowohl vom Internet als auch von Ihrem lokalen Netzwerk aus davon, dass das Programm ordnungsgemäß funktioniert.

5. Testen Sie die Firewall.

Prüfen Sie, nachdem Sie Ihre Firewall installiert und konfiguriert haben, ob sie ordnungsgemäß funktioniert. Testen Sie die Firewall, indem Sie versuchen, die blockierten Ports zu verwenden.

Absichern von Clustern

Systeme mit Clustern (also mit mehreren Servern) sind naturgemäß komplexer als Konfigurationen mit nur einem Server. Ein Acrobat Connect Pro-Cluster kann sich in einem Datenzentrum befinden oder über mehrere Netzwerkstandorte verteilt sein. Sie können Server, die Connect Pro hosten, an mehreren Standorten installieren und konfigurieren und über eine Datenbankreplikation synchronisieren.

Hinweis: *Cluster müssen anstelle der eingebetteten Datenbank-Engine Microsoft SQL Server Standard Edition verwenden.*

Nachstehend finden Sie einige wichtige Vorschläge zur Sicherung von Clustern:

Private Netzwerke Die einfachste Lösung für Cluster, die sich an einem einzigen Standort befinden, besteht darin, für das Acrobat Connect Pro-System ein zusätzliches Subnetzwerk einzurichten. Dieser Ansatz bietet eine hohe Sicherheitsstufe.

Lokale Software-Firewalls Wenn die Acrobat Connect Pro-Server sich in einem Cluster befinden, sich aber mit anderen Servern ein öffentliches Netzwerk teilen, bietet es sich an, für jeden einzelnen Server eine Software-Firewall einzurichten.

VPN-Systeme In Konfigurationen mit mehreren Servern, bei denen Acrobat Connect Pro an unterschiedlichen Standorten gehostet wird, sollte ein verschlüsselter Kanal für die Kommunikation mit den Remote-Servern in Erwägung gezogen werden. Zahlreiche Software- und Hardware-Hersteller bieten VPN-Technologien zur Sicherung

der Kommunikation mit Remote-Servern. Acrobat Connect Pro stützt sich auf diese externe Sicherheit, wenn der Datenverkehr verschlüsselt werden muss.

Sicherheitstipps und Ressourcen

Bewährte Sicherheitsvorkehrungen

Die folgende Checkliste beschreibt bewährte Methoden zur Sicherung Ihres Acrobat Connect Pro-Systems:

Schützen Sie Netzwerkverkehr durch SSL Sie können die Verbindung zum Meetingserver, zum Anwendungsserver oder zu beiden sichern.

Führen Sie nur die Dienste aus, die erforderlich sind Führen Sie keine Anwendungen wie einen Domain-Controller, Webserver oder FTP-Server auf demselben Computer wie Acrobat Connect Pro aus. Um die Wahrscheinlichkeit, dass eine andere Anwendung auf den Server gefährdende Weise genutzt werden kann, zu minimieren, verringern Sie die Anzahl an Anwendungen und Diensten auf dem Computer, der als Host für Acrobat Connect Pro dient.

Aktualisieren Sie die Sicherheitsfunktionen des Betriebssystems Überprüfen Sie regelmäßig, ob wichtige Updates für Sicherheitslücken vorliegen, und führen Sie die erforderlichen Patches aus. Eine Firewall kann einige dieser Sicherheitsprobleme aus der Welt schaffen. Im Allgemeinen sollten Sie stets darauf achten, dass die aktuellen Sicherheits-Patches von Microsoft und anderen relevanten Herstellern auf Ihren Servern installiert sind.

Sichern Sie die Hostsysteme Wenn Sie vertrauliche Informationen auf ihren Servern aufbewahren, sollten Sie dafür sorgen, dass die Hardware-Sicherheit Ihrer Systeme gewährleistet ist. Acrobat Connect Pro verlässt sich darauf, dass das Hostsystem ausreichende Schutzfunktionen gegen Eindringlinge bietet. Server sollten daher abgesichert werden, wenn private oder vertrauliche Daten in Gefahr sind. Acrobat Connect Pro kann native Umgebungsfunktionen wie etwa die Dateisystemverschlüsselung nutzen.

Verwenden Sie komplexe Kennwörter Gute Kennwörter tragen zum Datenschutz bei. Acrobat Connect Pro-Administratoren können Richtlinien für Anmeldenamen und Kennwörter in Connect Pro Central festlegen. Bei Acrobat Connect Pro-Installationen wird häufig Microsoft SQL Server 2005 Standard Edition eingesetzt. Auch hier sind komplexe Kennwörter erforderlich.

Verwenden Sie zur Authentifizierung LDAP oder Single-Sign-on Der Best-Practice-Ansatz sieht vor, die Authentifizierung für Connect Pro über LDAP oder Single-Sign-on zu realisieren. Falls Sie LDAP oder Single-Sign-on nicht verwenden, achten Sie darauf, dass die Endanwender nicht dasselbe Kennwort für Connect Pro verwenden, wie für andere Enterprise-Systeme.

Führen Sie regelmäßige Sicherheitsprüfungen durch Prüfen Sie Ihre Systeme in regelmäßigen Abständen, um die Funktionsfähigkeit aller Sicherheitsfunktionen zu gewährleisten. Sie können zum Beispiel mit einem Port-Scanner die Firewall testen.

Ressourcen und Informationsquellen in Bezug auf die Sicherheit

Die folgenden Ressourcen unterstützen Sie beim Absichern Ihrer Server:

Netzwerksicherheit Das SANS (System Administration, Networking and Security)-Institut ist eine kooperative Forschungs- und Bildungseinrichtung, der Systemadministratoren, Sicherheitsprofis und Netzwerkadministratoren angehören. Es bietet Kurse zum Thema Netzwerksicherheit sowie Zertifikate für die Netzwerksicherheit an.

SQL Server-Sicherheit Die Microsoft-Ressourcenseite zur SQL-Sicherheit auf der Microsoft-Website enthalten Informationen zum Sichern von SQL Server.

Werkzeuge NMap ist ein leistungsstarkes Port-Scanning-Programm, mit dem Sie feststellen können, welchen Port ein System gerade abhört. Es ist im Rahmen der GNU Public License (GPL) kostenlos verfügbar.

Hinweis: *Die Wirksamkeit jeder Sicherheitsmaßnahme ist von verschiedenen Faktoren abhängig, zum Beispiel von den Sicherheitsmaßnahmen, die der Server und die installierte Sicherheitssoftware bieten. Die Acrobat Connect Pro-Software wurde nicht entwickelt, um die Sicherheit Ihres Servers oder der darauf gespeicherten Informationen zu gewährleisten. Weitere Informationen finden Sie im Haftungsausschluss der zutreffenden Lizenzvereinbarung, die mit Acrobat Connect Pro geliefert wird.*

Kapitel 5: Administration von Connect Pro Server

Zur Administration von Acrobat Connect Pro Server gehören folgende Aufgaben:

- Verwalten und Überwachen von Protokolldateien, um Ausfallzeiten zu vermeiden
- Verwalten von Speicherplatz
- Sichern von Daten
- Zusammenstellen und Anfertigen von Nutzungsberichten

Starten und Beenden der Server

Starten und Beenden von Acrobat Connect Pro Server

Sie können Acrobat Connect Pro über das Start-Menü, über das Fenster „Dienste“ oder über die Befehlszeile starten oder beenden. Überprüfen Sie, dass die Datenbank ausgeführt wird, bevor Sie den Connect Pro Server starten.

Beenden von Acrobat Connect Pro über das Startmenü

1. Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server stoppen“.
2. Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server stoppen“.

Beenden von Acrobat Connect Pro über das Startmenü

1. Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Meeting Server starten“.
2. Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central Application Server starten“.

Beenden von Acrobat Connect Pro über das Fenster „Dienste“

1. Wählen Sie „Start“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“, um das Fenster „Dienste“ zu öffnen.
2. Beenden Sie den Dienst „Adobe Connect Enterprise Service“.
3. Beenden Sie den Dienst „Flash Media Server (FMS)“.
4. Beenden Sie den Dienst „Flash Media Administration Server“.

Starten von Acrobat Connect Pro über das Fenster „Dienste“

1. Wählen Sie „Start“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“, um das Fenster „Dienste“ zu öffnen.
2. Starten Sie den Dienst „Flash Media Server (FMS)“.
3. Starten Sie den Dienst „Flash Media Server Administration Server“.
4. Starten Sie den Dienst „Adobe Connect Enterprise Service“.

Beenden von Acrobat Connect Pro über die Befehlszeile

1 Wählen Sie „Start“ > „Ausführen“, um das Fenster „Ausführen“ zu öffnen. Geben Sie **cmd** ein, um eine Befehlszeile zu öffnen.

2 Wechseln Sie zum Verzeichnis „breeze\appserv\win32“.

3 Geben Sie folgenden Befehl ein, um Acrobat Connect Pro zu beenden:

```
net stop ConnectPro
```

4 Geben Sie Folgendes ein, um Flash Media Server zu beenden:

```
net stop FMS
```

5 Geben Sie Folgendes ein, um Flash Media Server Administration Server zu beenden:

```
net stop FMSAdmin
```

Starten von Acrobat Connect Pro über die Befehlszeile

1 Wählen Sie „Start“ > „Ausführen“, um das Fenster „Ausführen“ zu öffnen. Geben Sie **cmd** ein, um eine Befehlszeile zu öffnen.

2 Wechseln Sie zum Verzeichnis „breeze\appserv\win32“.

3 Geben Sie Folgendes ein, um Flash Media Server zu starten:

```
net start FMS
```

4 Geben Sie Folgendes ein, um Flash Media Server Administration Server zu starten:

```
net start FMSAdmin
```

5 Geben Sie Folgendes ein, um Acrobat Connect Pro zu starten:

```
net start ConnectPro
```

Starten und Beenden von Connect Pro Presence Service

Sie können Connect Pro Presence Service vom Startmenü oder vom Fenster „Dienste“ aus starten oder beenden. Starten Sie Connect Pro Presence Service nur, wenn Ihr Acrobat Connect Pro-System mit Microsoft Live Communications Server oder Office Communications Server integriert ist.

Verwandte Themen

„Integrieren mit Microsoft Live Communications Server 2005 und Microsoft Office Communications Server 2007“ auf Seite 54

Beenden des Presence Service vom Startmenü

❖ Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Pro Server 7“ > „Connect Pro Presence Service stoppen“.

Starten des Presence Service vom Startmenü

❖ Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Pro Server 7“ > „Connect Pro Presence Service starten“

Beenden, Starten oder Neustarten des Presence Service vom Fenster „Dienste“ aus.

1 Wählen Sie „Start“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“, um das Fenster „Dienste“ zu öffnen.

2 Wählen Sie Acrobat Connect Pro Presence Service.

3 Wählen Sie „Starten“, „Beenden“ oder „Neustarten des Dienstes“.

Starten und Anhalten von Flash Media Gateway

Sie können Flash Media Gateway entweder im Fenster „Dienste“ starten und beenden oder hierzu die Befehlszeile verwenden. Achten Sie darauf, dass Connect Pro Server ausgeführt wird, bevor Sie Flash Media Gateway starten.

Starten und Beenden von Flash Media Gateway im Fenster „Dienste“

1 Wählen Sie „Start“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“, um das Fenster „Dienste“ zu öffnen.

2 Wählen Sie den Dienst „Flash Media Gateway“ aus.

3 Wählen Sie Starten, Beenden oder Neustarten des Dienstes

Starten und Beenden von Flash Media Gateway über die Befehlszeile

1 Wählen Sie „Start“ > „Ausführen“, um das Fenster „Ausführen“ zu öffnen. Geben Sie **cmd** ein, um eine Befehlszeile zu öffnen.

2 Geben Sie folgenden Befehl ein, um Flash Media Gateway zu starten:

```
net start fmg
```

3 Geben Sie folgenden Befehl ein, um Flash Media Gateway zu beenden:

```
net stop fmg
```

Starten und Beenden von Acrobat Connect Pro Edge Server

Sie können Acrobat Connect Pro Edge Server 7 über das Start-Menü, über das Fenster „Dienste“ oder über die Befehlszeile starten oder beenden.

Beenden von Acrobat Connect Pro Edge Server 7 über das Startmenü

❖ Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Edge Server stoppen“.

Starten von Acrobat Connect Pro Edge Server 7 über das Startmenü

❖ Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Edge Server starten“.

Beenden von Acrobat Connect Pro Edge Server 7 über das Fenster „Dienste“

1 Wählen Sie „Start“ > „Einstellungen“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“, um das Fenster „Dienste“ zu öffnen.

2 Beenden Sie den Dienst „Flash Media Server (FMS)“.

3 Beenden Sie den Dienst „Flash Media Server Administration Server“.

Starten von Acrobat Connect Pro Edge Server über das Fenster „Dienste“

1 Wählen Sie „Start“ > „Einstellungen“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“, um das Fenster „Dienste“ zu öffnen.

2 Starten Sie den Dienst „Flash Media Server Administration Server“.

3 Starten Sie den Dienst „Flash Media Server (FMS)“.

Beenden von Acrobat Connect Pro Edge Server über die Befehlszeile

1 Wählen Sie „Start“ > „Ausführen“, um das Fenster „Ausführen“ zu öffnen. Geben Sie **cmd** ein, um eine Befehlszeile zu öffnen.

2 Geben Sie Folgendes ein, um Flash Media Server zu beenden:

```
net stop FMS
```

3 Geben Sie Folgendes ein, um Flash Media Server Administration Server zu beenden:

```
net stop FMSAdmin
```

Starten von Acrobat Connect Pro Edge Server über die Befehlszeile

1 Wählen Sie „Start“ > „Ausführen“, um das Fenster „Ausführen“ zu öffnen. Geben Sie **cmd** ein, um eine Befehlszeile zu öffnen.

2 Geben Sie Folgendes ein, um Flash Media Server Administration Server zu starten:

```
net start FMSAdmin
```

3 Geben Sie Folgendes ein, um Flash Media Server zu starten:

```
net start FMS
```

Verwalten und Überwachen von Protokolldateien

Informationen über Protokolldateien

Die Protokolldateien von Acrobat Connect Pro Server enthalten Informationen über Ereignisse, die während des Serverbetriebs auftreten. Sie können diese Informationen dazu verwenden, Überwachungsmechanismen und -berichte zu erstellen und Probleme zu beheben. Protokolldateien liefern Informationen zu Benutzeraktivitäten und Serverleistungen. Beispielsweise kann in Protokolldateien angegeben werden, warum Benutzern die Berechtigung zur Anmeldung verweigert wurde oder warum eine Telefonieverbindung nicht erfolgreich aufgebaut werden konnte.

Acrobat Connect Pro-Server enthält fünf Protokolldateien im Ordner *Stamm-Installationsverzeichnis\logs*. Mit den Dateien access.log und error.log können Sie Acrobat Connect Pro überwachen. Die anderen drei Protokolldateien sind intern und für den Betrieb des Systems nicht erforderlich.

access.log Enthält Informationen zu allen Zugriffsversuchen auf den Server.

breeze.log Enthält Informationen darüber, ob die Anwendung ConnectPro.exe gestartet wurde oder nicht.

error.log Enthält Informationen zu Systemproblemen.

service-err.log Enthält Anwendungs- und Startfehler.

service-out.log Enthält STDOUT und STDERR-Nachrichten, die die Java Virtual Machine generiert.

Beispieleintrag für eine Protokolldatei

Der folgende Beispieleintrag aus der Datei access.log umfasst eine Überschrift, eine Liste der im Protokolleintrag verwendeten Felder und die spezifischen Daten für den Protokolleintrag:

```
#Version: 1.0
#Start-Date: 2006-10-30 17:09:24 PDT
#Software: Adobe Acrobat Connect Pro Server 7
#Date: 2006-04-30
#Fields: date time x-comment x-module x-status x-severity x-category x-user x-access-request
time-taken db-logical-io db-transaction-update-count
2006-10-30 18:12:50 Not logged in. PRINCIPAL NO_ACCESS_NO_LOGIN W A PUBLIC
{cookie=breezxnb5pqusyshfgttt, ip=138.1.21.100} GET http://joeuser.macromedia.com&mode=xml 0
20/5 0
```

In der folgenden Tabelle wird der Beispieleintrag erläutert:

Feld	Daten	Beschreibung
date	2006-10-30	Das Datum, an dem das protokollierte Ereignis eingetreten ist.
time	18:12:50	Die Uhrzeit, zu der das protokollierte Ereignis eingetreten ist.
x-comment	Nicht angemeldet.	Gibt an, dass ein Benutzer sich nicht beim Abwendungsserver anmelden konnte.
x-module	PRINCIPAL	Das Ereignis ist im Modul PRINCIPAL im Abwendungsserver aufgetreten.
x-status	NO_ACCESS_NO_LOGIN	Gibt an, dass der Benutzer sich nicht anmelden konnte.
x-serverity	W	Gibt als Schweregrad des Ereignisses Warnung (W) an.
x-category	A	Gibt an, dass es sich bei dem Ereignis um ein Zugriffsproblem (A) handelt, das in der Datei access.log angezeigt wird.
x-user	PUBLIC	Der aktuelle Benutzer. In diesem Fall ein nicht identifizierter Gast oder ein öffentlicher Benutzer.
x-access-request	http://maxmustermann.adobe.com&mode=xml	Quelle der Anforderung.
time-taken	0	Zur Ausführung dieser Anforderung wurde keine Zeit benötigt.
db-logical-io	20/5	Es waren 20 Lesevorgänge in der Datenbank nötig und 5 Datenzeilen wurden zurückgegeben.
db-transaction-update-count	0	Bei der Verarbeitung dieser Anforderungen wurden keine Datenbankzeilen aktualisiert.

Wechseln zwischen Protokolldateien

Sie können die Dateien access.log und error.log wechseln. Ändern Sie die Standardwerte der folgenden Parameter in der Datei custom.ini (standarmäßig unter *Stamm-Installationsverzeichnis*\custom.ini), um festzulegen, wie häufig die Protokolldateien gewechselt werden:

```
ACCESS_LOG_ROTATE_DAYS=1.0
ACCESS_LOG_ROTATE_KEEP=7
ERROR_LOG_ROTATE_DAYS=1.0
ERROR_LOG_ROTATE_KEEP=7
```

Die Parameter `*_DAYS` legen fest, wie häufig die Protokolldateien gewechselt werden (in Tagen). Der Wert 0,5 steht für einen halben Tag.

Die Parameter `*_KEEP` legen fest, wie viele Tage die Protokolldateien aufbewahrt werden, bevor Sie gelöscht werden. Standardmäßig werden die Protokolldateien eine Woche lang aufbewahrt.

Nachdem Sie die Datei custom.ini geändert haben, starten Sie den Connect Pro Central-Anwendungsserver neu.

Protokolldateiformat

Die Protokolldateien verwenden das erweiterte Protokolldateiformat des W3C, das von allen Text-Editoren gelesen werden kann.

Protokollfelder in den Dateien access.log und·error.log

Die einzelnen Protokolleinträge enthalten 11 Protokollfelder. Sie liefern Informationen über Art und Ort des aufgetretenen Ereignisses, über den Schweregrad und andere relevanten Daten:

Feld	**Format**	**Beschreibung**
date	JJJJ/MM/TT	Tag der Ausführung der Transaktion,
time	HH:MM:SS	Lokale Computerzeit, zu der die Transaktion ausgeführt wurde.
x-comment	Zeichenfolge	Enthält lesbare Informationen zum Protokolleintrag. Dieses Feld wird immer ganz links ausgegeben.
x-module	Zeichenfolge	Gibt an, wo der Fehler aufgetreten ist.
x-status	Zeichenfolge	Gibt an, welches Ereignis aufgetreten ist.
x-serverity	Text (ein Zeichen)	Gibt an, ob das protokollierte Ereignis kritisch (C), Fehler (E), Warnung (W) oder Information (I) ist.
x-category	Text (ein Zeichen)	Gibt an, ob der Protokolleintrag ein Zugriffsereignis (A) oder Systemereignis (S) darstellt.
x-user	Zeichenfolge	Text, der den aktuellen Benutzer angibt. Nur anwendbar, wenn x-category Zugriff (A) ist, andernfalls ist Feld auf einen Bindestrich (-) für „nicht verwendetes Feld“ eingestellt.
x-access-request	Zeichenfolge	Text, der die Zugriffsanforderung darstellt. Es kann sich um eine URL oder einen API-Namen mit übergebenen Parametern handeln. Nur anwendbar, wenn x-category Zugriff (A) ist, andernfalls ist Feld auf einen Bindestrich (-) für „nicht verwendetes Feld“ eingestellt.
time-taken	Nummer	Zeit, die zur Verarbeitung der Anforderung erforderlich ist (in Sekunden). Nur anwendbar, wenn x-category Zugriff (A) ist, andernfalls ist Feld auf einen Bindestrich (-) für „nicht verwendetes Feld“ eingestellt.
db-logical-io	Zeichenfolge	Anzahl der Lesevorgänge in der Datenbank, die erforderlich sind, um die Anforderung zu verarbeiten und die Anzahl der im Format <reads>/<rows> zurückgegebenen Zeilen.
db-transaction-update-count	Zeichenfolge	Anzahl der in Transaktionen aktualisierten Zeilen beim Verarbeiten der Anforderungen. Wenn die Anforderung mehrere Transaktionen verwendet, ist dieser Wert die Summe aller Aktualisierungen.

Modulfeldeinträge

Ein Modul ist eine Komponente des Servers, die einige verbundene Vorgangssätze verwaltet. Die einzelnen Module gehören entweder zum Abwendungsserver oder zum Meetingserver. Das Feld x-module gibt an, wo das Protokollereignis aufgetreten ist:

x-module	**Beschreibung**	**Server**
ACCESS_KEY	Verwaltet Zugriffstasten	Anwendungsserver
ACCOUNT	Verwaltet Kontenvorgänge	Anwendungsserver
ACL	Verwaltet ACL-bezogene Vorgänge	Anwendungsserver
AICC	Verwaltet alle AICC-Kommunikationen zwischen Server und Materialien	Anwendungsserver
BUILDER	Führt SCO-Builds aus	Anwendungsserver
Client	Client-Methoden.	Meetingserver
CLUSTER	Verwaltet alle clusterbezogenen Vorgänge	Anwendungsserver
CONSOLE	Verwaltet alle konsolenbezogenen Vorgänge	Anwendungsserver
Content	Freigabe-Pod.	Meetingserver
DB	Stellt die Datenbank dar	Anwendungsserver
EVENT	Verwaltet alle veranstaltungsbezogenen Vorgänge	Anwendungsserver

x-module	Beschreibung	Server
HOSTED_MANAGER	Verwaltet Systemkonten (erstellen, aktualisieren, löschen, Einstellungen usw.)	Anwendungsserver
MEETING	Verwaltet alle meetingbezogenen Vorgänge	Anwendungsserver
Misc	Verschiedene Module	Meetingserver
NOTIFICATION	Verwaltet alle E-Mail-Vorgänge.	Anwendungsserver
PERMISSION	Verwaltet alle berechtigungsbezogenen Vorgänge	Anwendungsserver
Poll	Abstimmungs-Pod.	Meetingserver
PLATFORM_FRAMEWORK	Stellt das Plattform-Framework dar	Anwendungsserver
PRINCIPAL	Verwaltet alle Principal-bezogenen Vorgänge	Anwendungsserver
REPORT	Stellt Berichte dar	Anwendungsserver
Room	Verwaltet das Hoch- und Herunterfahren von Meetingräumen	Meetingserver
RTMP	Stellt den RMTPHandler dar	Anwendungsserver
SCO	Verwaltet alle SCO-bezogenen Vorgänge	Anwendungsserver
SEARCH	Verwaltet alle suchbezogenen Vorgänge	Anwendungsserver
START_UP	Stellt die Startkomponente dar	Anwendungsserver
TELEPHONY	Verwaltet alle telefoniebezogenen Vorgänge	Anwendungsserver
TRACKING	Verwaltet alle telefoniebezogenen Vorgänge	Anwendungsserver
TRAINING	Verwaltet alle schulungsbezogenen Vorgänge	Anwendungsserver

Kommentar- und Statusfeldeinträge

Die Felder x-comment und x-status geben an, welche Art von Ereignis aufgetreten ist. Das Feld x-status liefert einen Code für die einzelnen protokollierten Ereignisse. Das Feld x-comment liefert eine lesbare Beschreibung der einzelnen protokollierten Ereignisse.

In der folgenden Tabelle sind die Statuscodes, die den Statuscodes zugeordneten Kommentare und jeweils eine Erläuterung der protokollierten Ereignisse aufgeführt:

Protokolleintrag für x-status-Feld	Protokolleintrag für x-comment-Feld	Beschreibung
ACCESS_DENIED	Client trying to access protected method Access is denied. {1}	Wird eingetragen, wenn der Client versucht, auf eine geschützte Methode zuzugreifen.
BECAME_MASTER	Server {1} has been designated the master.	Wird eingetragen, wenn der Scheduler beendet und dieser Server zum Scheduler wird.
CLUSTER_CON_BROKEN	Server {1} unable to reach {2} on port {3} to perform cluster operations.	Wird eingetragen, wenn Acrobat Connect Pro keinen anderen Server im Cluster erreichen kann.
CLUSTER_FILE_TRANSFER_ERROR	Unable to transfer {1} from server {2}.	Wird eingetragen, wenn beim Übertragen einer Datei ein Fehler ausgegeben wird.
CONNECT	New client connecting: {1}	Wird eingetragen, wenn sich ein neuer Client anmeldet.

Protokolleintrag für x-status-Feld	**Protokolleintrag für x-comment-Feld**	**Beschreibung**
CONNECT_WHILE_GC	Connecting while the application is shutting down - forcing shutdown.	Wird eingetragen, wenn der Client versucht sich anzumelden, während die Anwendung heruntergefahren wird.
DB_CONNECTION_ERROR	Unable to connect to database {1}.	Wird eingetragen, wenn Acrobat Connect die Datenbank nicht erreichen kann.
DB_CONNECTION_TIME_OUT	Timed out waiting for database connection.	Wird eingetragen, wenn die Zeit zur Herstellung der Datenbankverbindung abgelaufen ist.
DB_VERSION_ERROR	Database {1} is incompatible with the current version of Acrobat Connect Pro.	Wird eingetragen, wenn die Datenbank nicht mehr aktuell ist.
DISCONNECT	A client is leaving. Details: {1}	Wird eingetragen, wenn sich ein Client abmeldet.
EXT_ERROR	External error thrown by a third party.	Wird eingetragen, wenn ein externer Code einen Fehler verursacht.
FMS_CON_BROKEN	Health check failed due to broken FMS service connection.	Wird eingetragen, wenn die Serviceverbindung erschwert ist.
FMS_NOT_FOUND	Unable to connect to FMS at startup.	Wird eingetragen, wenn Acrobat Connect beim Start keine Serviceverbindung einrichten kann.
INTERNAL_ERROR	Internal error occurred.	Wird eingetragen, wenn ein interner Fehler ausgegeben wird.
INVALID	-	Wird eingetragen, wenn versucht wird, einen ungültigen Vorgang auszuführen.
INVALID_DUPLICATE	Value {1} is a duplicate in the system.	Wird eingetragen, wenn der eingegebene Wert im System bereits vorhanden ist.
INVALID_FORMAT	Field {1} of type {2} is invalid.	Der angegebene Wert ist für dieses Feld ungültig.
INVALID_ILLEGAL_OPERATION	Illegal operation performed.	Der angeforderte Vorgang ist nicht zulässig.
INVALID_	-	Wird eingetragen, wenn ACL ein ungültiger Wert übergeordnet ist. Beispiel: Wenn sich Ordner A in Ordner B befindet, kann sich Ordner B sich nicht in Ordner A befinden.
INVALID_MISSING	Field {1} of type {2} is missing.	Der für dieses Feld erforderliche Wert fehlt.
INVALID_NO_SUCH_ITEM	Value {1} is an unknown in the system.	Das angeforderte Element ist nicht vorhanden.
INVALID_RANGE	The specified value must be between {1} and {2}.	Wird eingetragen, wenn der eingegebene Wert außerhalb des gültigen Bereichs liegt.
INVALID_TELEPHONY_FIELD	Telephony authentication values were not validated by the service provider.	Service-Anbieter kann das Telefonkonto nicht validieren.
INVALID_VALUE_GTE	The specified value must be greater than or equal to {1}.	Wird eingetragen, wenn der eingegebene Wert außerhalb des gültigen Bereichs liegt.

Protokolleintrag für x-status-Feld	Protokolleintrag für x-comment-Feld	Beschreibung
INVALID_VALUE_LTE	The specified value must be less than or equal to {1}.	Wird eingetragen, wenn der eingegebene Wert außerhalb des gültigen Bereichs liegt.
KILLING_LONG_CONNECTION	Client has been in the room for 12 hours, disconnecting.	Wird eingetragen, wenn die Client-Verbindung nach Erreichen des Zeitlimits abgebrochen wird.
LICENSE_EXPIRED	Your license has expired and your account will be disabled on {1}. Please upload a new license file through the console manager to continue using Acrobat Connect Pro.	Wird eingetragen, wenn Acrobat Kunden Connect Pro während der Toleranzfrist verwenden und der Zugriff bald abläuft.
LICENSE_EXPIRY_WARNING	Your license will expire on {1}. Please upload a new license file through the console manager to continue using Acrobat Connect Pro.	Wird eingetragen, wenn die Lizenz in 15 Tagen oder weniger abläuft.
MASTER_THREAD_TIMED_OUT	Master thread has not reported progress in {1} milliseconds.	Der Thread des Schedulers wird nicht ausgeführt.
MEETING_BACKUP_END	Server {1} is no longer the backup for room {2}.	Das Backup des Meetings ist abgeschlossen.
MEETING_BACKUP_START	Server {1} is now the backup for room {2}.	Das Backup des Meetings wurde gestartet.
MEETING_FAILOVER	Meeting {1} failed over to {2}.	Wird eingetragen, wenn ein Meeting ausfällt und auf diesem Server ausgeführt wird.
MEETING_TMP_READ	Meeting template {1} read for room {2}.	Vorlage von Meeting gelesen.
MEETING_TMP_WRITTEN	Meeting template {1} written to room {2}.	Vorlage in Meeting geschrieben.
NO_ACCESS_ACCOUNT_EXPIRED	Your account has expired.	Das Konto, auf das zugegriffen wird, ist abgelaufen.
NO_ACCESS_DENIED	Permission check failed.	Fehler bei der Berechtigungsprüfung.
NO_ACCESS_LEARNER	No permission to take courses.	Um an einem Kurs teilnehmen zu können, müssen Sie ein Mitglied der Teilnehmergruppe sein.
NO_ACCESS_LEARNING_PATH_BLOCKED	You have not fulfilled a prerequisite or preassessment.	Voraussetzungs- oder Einstufungsfehler
NO_ACCESS_NO_EXTERNAL_USER_MODIFICATION	External users cannot be modified.	Benutzer können LDAP-Benutzer nicht modifizieren.
NO_ACCESS_NO_LICENSE_FILE	Your license file has not been uploaded.	Die Lizenzdatei wurde nicht gefunden.
NO_ACCESS_NO_LOGIN	Not logged in.	Fehler wird ausgegeben, wenn ein Benutzer nicht angemeldet ist.
NO_ACCESS_NO_LOGIN	A {1} quota error occurred for account {2} with limit {3}.	Außerhalb der Quote.
NO_ACCESS_NO_RETRY	You have reached the max limit and can not take the course again.	Benutzer hat die Grenze für maximale Kurswiederholungen erreicht.
NO_ACCESS_NO_SERVER	Server not available	Der angeforderte Server ist nicht verfügbar.
NO_ACCESS_NOT_AVAILABLE	The requested resource is unavailable.	Wird eingetragen, wenn die angeforderte Ressource nicht verfügbar ist.

Protokolleintrag für x-status-Feld	Protokolleintrag für x-comment-Feld	Beschreibung
NO_ACCESS_NOT_SECURE	SSL request made on a non-SSL server.	Sichere Anforderung auf nicht sicherem Server ausgeführt.
NO_ACCESS_PASSWORD_EXPIRED	Your password has expired.	Wird eingetragen, wenn das Benutzerkennwort abgelaufen ist.
NO_ACCESS_PENDING_ACTIVATION	Your account has not been activated yet.	Benutzerkonto noch nicht aktiviert.
NO_ACCESS_PENDING_LICENSE	Your account activation is pending a license agreement.	Konto erst verwendbar, wenn Lizenzvereinbarung gelesen wurde.
NO_ACCESS_SCO_EXPIRED	The course you tried to access is no longer available.	Das Enddatum des Kurses ist abgelaufen.
NO_ACCESS_SCO_NOT_STARTED	Course is not open yet.	Das Startdatum des Kurses ist noch nicht erreicht.
NO_ACCESS_WRONG_ZONE	Content accessed from wrong zone.	Wird ausgelöst, wenn Materialien oder Benutzer in der falschen Zone auf einen Server zugreifen.
NO_DATA	Permission check failed.	Abfrage gab keine Daten zurück.
NO_DISKSPACE	Health check failed due to lack of disk space.	Wird eingetragen, wenn für das Konto kein Platz auf der Platte vorhanden ist.
NOT_AVAILABLE	Requested resource is not available.	Fehler wird ausgegeben, wenn Ressource nicht verfügbar ist.
OK	-	Anforderung wurde erfolgreich verarbeitet.
OPERATION_SIZE_ERROR	Operation too large to complete.	Wird eingetragen, wenn der Vorgang aufgrund der Größe nicht ausgeführt werden kann.
REQUEST_RETRY	Unable to process request. Please try again.	Die Anforderung ist fehlgeschlagen.
RESPONSE_ABORTED	Client that made request is not available to receive response.	Wird eingetragen, wenn Benutzer Browser schließt, bevor Server Antwort zurücksenden kann.
RTMP_SVC_BLOCKED	Acrobat Connect Pro service request blocked from {1} because the server has not fully started up yet.	Serviceverbindung von SCO angefordert, der Server wird jedoch noch hochgefahren.
RTMP_SVC_CLOSED	Acrobat Connect Pro service connection closed for {1}.	Serviceverbindung für SCO geschlossen.
RTMP_SVC_REQUEST	Acrobat Connect Pro service request received from {1}.	Serviceverbindung von SCO angefordert.
RTMP_SVC_START	Acrobat Connect Pro service connection established with {1}.	Serviceverbindung mit SCO eingerichtet.
SCRIPT_ERROR	Run-Time Script Error. Details: {1}	Wird eingetragen, wenn ein Skriptfehler erkannt wird.
SERVER_EXPIRED	Health check failed due to server expiry (expiry date={1}, current time={2}).	Wird eingetragen, wenn Gesundheitsprüfung für Server nicht erfolgreich ausgeführt werden kann, bevor Zeit abläuft.
SOME_ERRORS_TERMINATED	Some actions terminated with an error.	Wird eingetragen, wenn einige Aktionen durch einen Fehler abgebrochen werden.

Protokolleintrag für x-status-Feld	**Protokolleintrag für x-comment-Feld**	**Beschreibung**
START_UP_ERROR	Start up error: {1}.	Wird eingetragen, wenn während des Starts eine Ausnahme ausgelöst wird.
START_UP_ERROR_UNKNOWN	Unable to start up server. Acrobat Connect Pro might already be running.	Wird eingetragen, wenn während des Starts ein unbekannter Fehler ausgegeben wird. JRUN druckt den Fehler aus.
TEL_CONNECTION_BROKEN	Telephony connection {1} was unexpectedly broken.	Wird eingetragen, wenn die Telefonieverbindung unterbrochen wird.
TEL_CONNECTION_RECOVERY	Telephony connection {1} was reattached to conference {2}.	Wird eingetragen, wenn Acrobat Connect eine erneute Verbindung zur Konferenz wiederherstellt.
TEL_DOWNLOAD_FAILED	Unable to download {1} for archive {2}.	Wird eingetragen, wenn beim Herunterladen von Telefonieaudiodateien die Zeit abläuft.
TOO_MUCH_DATA	Multiple rows unexpectedly returned.	Wird eingetragen, wenn ein Vorgang mehr Daten zurückgibt als erwartet.
UNKNOWN_TYPE	{1}	Wird eingetragen, wenn der Typ der Variablen nicht bekannt ist.

Hinweis: *In der vorhergehenden Tabelle sind {1} und {2} Variablen, die im Protokolleintrag durch einen Wert ersetzt werden.*

Einträge in die Felder zum Schweregrad

Das Feld x-serverity gibt an, wie ernst eine Situation ist, sodass Sie die entsprechende Reaktion festlegen können.

Protokolleintrag für x-serverity	**Bedeutung**	**Vorgeschlagene Aktion**	**Beispiel**
C	Kritisch	Überwachungswerkzeuge von Drittanbietern konfigurieren, um Pager zu warnen, wenn ein Protokolleintrag mit diesem Schweregrad auftritt.	Eine Verbindung zur Datenbank kann nicht hergestellt werden. Ein Prozess kann nicht gestartet oder beendet werden. Im System ist ein Fehler aufgetreten.
E	Fehler	Überwachungswerkzeuge von Drittanbietern konfigurieren, um E-Mail-Nachricht zu senden, wenn ein Protokolleintrag mit diesem Schweregrad auftritt.	Verbindung zu Adobe® Premiere® kann nicht hergestellt werden. Konvertierung konnte nicht erfolgreich durchgeführt werden. Ein Fehler betrifft den Benutzer oder Konto, jedoch nicht das gesamte System.
W	Warnungen	Berichte in regelmäßigen Abständen generieren und prüfen, um mögliche Betriebs- und Produktverbesserungen zu identifizieren.	Platten- oder Speicherauslastung überschreitet den angegebenen Schwellenwert.
I	Info	Protokolleinträge zu Auditing- oder RCA-Zwecken überprüfen	Server gestartet, gestoppt oder neu gestartet.

Kategoriefeldeinträge

Das Feld x-category gibt an, ob sich das Ereignis auf Zugriffsprobleme (A) oder allgemeine Systemprobleme (S) bezieht. Alle Einträge der Kategorie A werden in der Datei access.log angegeben und alle Einträge der Kategorie S, werden in der Datei error.log angezeigt.

Protokolleintrag für x-category-Feld	Bedeutung	Beschreibung
A	Access (Zugriff)	Statuscode bezieht sich auf Zugriffsprobleme. Eingetragen in Datei „access.log“.
S	System	Statuscode bezieht sich auf allgemeine Systemprobleme. Eingetragen in Datei error.log.

Verwalten von Speicherplatz

Informationen über Speicherplatzverringerung

Das Acrobat Connect Pro-System muss über mindestens 1 GB freien Speicherplatz verfügen. Acrobat Connect Pro verfügt nicht über integrierte Tools zur Überwachung des Speicherplatzes auf der Festplatte - der Administrator muss den Speicherplatz mit Anwendungen des Betriebssystems oder von Drittanbietern selbst überwachen.

Materialien können auf dem Hostserver von Acrobat Connect Pro und/oder auf externen gemeinsamen Speichervolumen gespeichert werden.

Verwandte Themen

„Konfigurieren von gemeinsamem Speicher“ auf Seite 48

Verwalten von Speicherplatz auf Acrobat Connect Pro-Servern

❖ Führen Sie einen der folgenden Schritte aus:

- Nutzen Sie Connect Pro Central zum Löschen ungenutzer Materialien. Weitere Informationen finden Sie unter Löschen von Dateien oder Ordnern.
- Tauschen Sie Ihre Serverfestplatte gegen eine größere aus.

Hinweis: *Wenn weniger als 1 GB Speicherplatz frei ist, kann der Server nicht ausgeführt werden.*

Verwalten von Speicherplatz auf freigegebenen Speichergeräten

❖ Überwachen Sie das gemeinsamen Hauptspeichergerät auf freien Speicherplatz und verfügbare Datei-Systemknoten hin. Fällt eines davon auf unter 10 %, stellen Sie mehr Speicherplatz auf dem Gerät bereit oder fügen Sie ein weiteres gemeinsames Speichergerät hinzu.

Hinweis: *10 % ist ein empfohlener Wert. Legen Sie bei der Verwendung gemeinsamen Speichers außerdem in der Anwendungsverwaltungskonsole eine Maximalgröße für den Cache fest, ansonsten kann der Cache die Festplatte füllen.*

Leeren des Edge Server-Cache

Adobe empfiehlt die wöchentliche Leerung des Edge Server-Cache. Führen Sie die Aufgabe außerhalb der Spitzenauslastungszeiten aus, zum Beispiel am frühen Sonntag morgen.

1 Erstellen Sie eine Datei cache.bat zum Löschen des Cache-Verzeichnisses. Der Befehl in dieser Datei muss folgende Syntax aufweisen:

```
del /Q /S [cache directory]\*.*
```

Standard-Cache-Verzeichnis C:\\breeze\\edgeserver\\win32\\cache\\http. Löschen Sie den Cache mit dem folgenden Befehl:

```
del /Q /S c:\breeze\edgeserver\win32\cache\http\*.*
```

2 Wählen Sie „Start“ > „Programme“ > „Adobe Connect Pro Edge Server 7“ > „Adobe Connect Pro Edge Server stoppen“

3 Führen Sie die Datei cache.bat aus, um zu überprüfen, ob das Cache-Verzeichnis gelöscht wird.

Hinweis: *Die Verzeichnisstruktur bleibt erhalten und alle Dateien, die der Edge-Server sperrt, werden nicht gelöscht.*

4 Wählen Sie „Start“ > „Programme“ > „Adobe Connect Pro Edge Server 7“ > „Adobe Connect Pro Edge Server starten“.

5 Wählen Sie „Start“ > „Systemsteuerung“ > „Geplante Tasks“ > „Geplanten Task hinzufügen“.

6 Wählen Sie cache.bat als neue auszuführende Datei aus.

7 Wiederholen Sie diese Schritte für jeden Edge-Server.

Sichern von Daten

Informationen zur Datensicherung

Es gibt drei Arten von Daten, die Sie regelmäßig sichern müssen: Materialien (alle Dateien, die in den Bibliotheken gespeichert sind), Konfigurationseinstellungen und Datenbank-Daten.

Wenn Sie keine gemeinsamen Speichergeräte nutzen, werden alle Materialien aus Bibliotheken im *Stamm-Installationsverzeichnis* \Materialordner gespeichert (standardmäßig C:\breeze\content). Die Konfigurationseinstellungen sind in der Datei custom.ini im Stamm-Installationsverzeichnis (standardmäßig C:\breeze) gespeichert.

Bei einer Datenbanksicherung wird ein Duplikat der Daten in der Datenbank erstellt. Regelmäßig durchgeführte Datenbanksicherungen helfen Ihnen bei der Wiederherstellung im Fall von defekten Speichermedien, Benutzerfehlern oder permanentem Serverausfall. Erstellen Sie täglich eine Sicherungskopie der Datenbank.

Sie können Sicherungskopien auch nutzen, um eine Datenbank von einem Server auf den anderen zu kopieren. Sie können eine gesamte Datenbank aus der Sicherungskopie in einem Schritt wiederherstellen. Beim Wiederherstellungsvorgang wird die bestehende Datenbank überschrieben bzw. eine neue Datenbank erstellt, wenn diese noch nicht existiert. Die wieder hergestellte Datenbank entspricht dem Datenbankzustand zum Zeitpunkt der Sicherung abzüglich jeglicher nicht durchgeführter Transaktionen.

Sicherungskopien werden auf Sicherungsgeräten, wie zum Beispiel Festplatten oder Bändern, erstellt. Sie können ein SQL Server-Dienstprogramm zur Konfiguration Ihrer Sicherungskopien nutzen. So können Sie etwa veraltete Sicherungskopien überschreiben oder neue Sicherungskopien an die Sicherungsmedien anfügen.

Greifen Sie bei der Sicherung einer Datenbank auf bewährte Methoden zurück:

- Legen Sie den Sicherungstermin in die Nacht.
- Bewahren Sie Sicherungskopien an einem sicheren Ort auf, vorzugsweise an einem anderen Ort als dem, an dem sich die Daten befinden.
- Bewahren Sie ältere Sicherungskopien für einen gewissen Zeitraum auf, für den Fall, dass die aktuelle Sicherungskopie beschädigt, zerstört oder verloren ist.
- Richten Sie ein System zum Überschreiben von Sicherungskopien ein und nutzen Sie dabei die ältesten Kopien zuerst. Nutzen Sie Ablaufdaten für Sicherungskopien, um ein vorzeitiges Überschreiben zu vermeiden.
- Beschriften Sie Sicherungsmedien, um das Datum festzuhalten und sicherzustellen, dass wichtige Sicherungen nicht überschrieben werden.

  Nutzen Sie SQL Server-Dienstprogramme, um die Datenbank zu sichern:

- Transact-SQL
- SQL Distributed Management Objects
- Assistent zur Erstellung von Datenbanksicherungen
- SQL Server Management Studio

Sichern von Serverdateien

Sichern und schützen Sie Systemdaten wie alle wertvollen Vermögenswerte Ihres Unternehmens.

Am besten lässt sich dies nachts erledigen.

1 Führen Sie folgende Schritte aus, um Acrobat Connect Pro zu beenden:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central-Dienst stoppen“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Meeting-Dienst stoppen“.

2 Erstellen Sie eine Sicherungskopie des Materialverzeichnisses.

Das Standardverzeichnis ist c:\breeze.

3 Erstellen Sie eine Sicherungskopie der Datei „custom.ini“.

Das Standardverzeichnis ist c:\breeze\.

4 Führen Sie folgende Schritte aus, um Acrobat Connect Pro zu starten:

a Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Meeting-Dienst starten“.

b Wählen Sie „Start“ > „Programme“ > „Adobe Acrobat Connect Pro Server 7“ > „Connect Pro Central-Dienst starten“.

Sichern der Datenbank

Eine Datensicherung beliebiger Versionen von Microsoft SQL Server können Sie mit Microsoft SQL Server Management Studio oder mit dem Befehlszeilenfenster anfertigen.

SQL Server Management Studio ist in der mit Connect Pro Server gelieferten Version von SQL Server nicht enthalten. Sie können die Software jedoch von Microsoft unter folgender Internetadresse herunterladen: Microsoft SQL Server Management Studio Express.

Verwenden von SQL Server Management Studio zur Datensicherung von SQL Server

***Wichtig:** Deinstallieren Sie die Datenbank nicht.*

1 Wählen Sie unter Windows „Start“ > „Programme“ > „Microsoft SQL Server 2005“ > „SQL Server Management Studio“.

2 Klicken Sie in der Strukturansicht des Objektexplorerfensters mit der rechten Maustaste auf die Datenbank (Standardname: „Breeze“) und wählen Sie die Option „Tasks“ > „Sichern...“.

***Hinweis:** Ausführliche Anleitungen zum Sichern und Wiederherstellen der SQL Server-Datenbank finden Sie auf der Support-Website von Microsoft.*

Verwenden des Befehlszeilenfensters zur Datensicherung von SQL Server

Durch Eingabe von `osql ?` in der DOS-Befehlszeile und anschließendes Drücken der Eingabetaste können Sie Informationen zu den Datenbankbefehlen aufrufen.

***Wichtig:** Deinstallieren Sie die Datenbank nicht.*

1 Melden Sie sich an dem Server an, der als Host für Connect Pro Server dient.

2 Erstellen Sie einen Ordner, in dem die Sicherungsdateien der Datenbank gespeichert werden sollen.

In diesem Beispiel wird der Ordner „C:\Connect_Database“ verwendet.

3 Wählen Sie „Start“ > „Ausführen“, geben Sie im Feld „Öffnen“ **cmd** ein und klicken Sie auf „OK“.

4 Wechseln Sie an der Befehlszeile zu dem Verzeichnis, in dem Sie die Datenbank installiert haben. Standardmäßig wird das Verzeichnis C:\Program Files\Microsoft SQL Server\90\Tools\Binn verwendet.

5 Geben Sie in der Befehlszeile **osql -E** ein, um sich an der Datenbankengine anzumelden, und drücken Sie Eingabe.

6 Geben Sie **BACKUP DATABASE database-name TO DISK = 'C:\Connect_Database\database-name.bak'** ein, um ein Microsoft SQL-Dienstprogramm auszuführen, das die Connect-Datenbank sichert, und drücken Sie die Eingabetaste.

Der Standardname lautet *breeze*.

7 Geben Sie an der Eingabeaufforderung den Befehl **go** ein und drücken Sie die Eingabetaste.

Im Befehlsfenster werden Nachrichten zur Sicherung angezeigt.

8 Geben Sie an der Eingabeaufforderung den Befehl **quit** ein und drücken Sie die Eingabetaste.

9 Um zu überprüfen, ob die Sicherung erfolgreich war, stellen Sie sicher, dass die Datei „breeze.bak“ im Verzeichnis „C:\Connect_Database“ vorhanden ist.

10 Um die Datenbank neu zu starten, wählen Sie im Windows-Desktop „Start“ > „Systemsteuerung“ > „Verwaltung“ > „Dienste“. Klicken Sie im Dialogfeld „Dienste“ mit der rechten Maustaste auf SQL Server (MSSQLSERVER) und wählen Sie im Kontextmenü „Starten“.

Erstellen benutzerdefinierter Berichte

Erstellen von benutzerdefinierten Berichten mit Star-Schemaansichten

Acrobat Connect Pro speichert Informationen zu Benutzern, Materialien, Kursen und Meetings in einer Datenbank. Die Benutzeraktivität füllt die Datenbank mit Daten. Mit Werkzeugen wie Adobe® ColdFusion® Studio und Business Objects Crystal Reports können Sie Star-Schemaansichten abfragen und die Daten anzeigen. Sie können auch SQL-basierte Werkzeuge wie SQL Query Analyzer verwenden.

Die folgenden Acrobat Connect Pro-Anwendungen können Daten in Berichte ausgeben:

Acrobat Connect Pro Meeting Meetingteilnehmer, Meetingdauer und Meetingmaterialien

Adobe Presenter Materialansichten, Folienansichten und Präsentationsansichten

Acrobat Connect Pro Schulung Informationen zur Kursverwaltung wie Statistiken zu den Kursteilnehmern, Statistiken zur Materialanzeige und Quizergebnisse

Hinweis: *Darüber hinaus können Sie Berichte von der Webanwendung Connect Pro Central ausführen und sie im CSV-Format anzeigen oder herunterladen. Weitere Informationen hierzu finden Sie unter* *Erstellen von Berichten in Connect Pro Central*.

SCO-Fakt

Spalte	Beschreibung
dim_sco_details_sco_id	Sco-ID
dim_sco_details_sco_version	SCO-Version
max_retries	Maximale Anzahl von Wiederholungen
owner_user_id	Benutzer-ID des SCO-Eigentümers
disk_usage_kb	Plattenauslastung in Kilobyte
passing_score	Punktzahl (bestanden)
max_possible_score	Höchst mögliche Punktzahl
views	Anzeigehäufigkeit
unique_viewers	Anzahl der eindeutigen Benutzer, die SCO angezeigt haben
slides	Anzahl der Folien
questions	Anzahl der Fragen
max_score	Höchstpunktzahl
min_score	Mindestpunktzahl
average_score	Durchschnittliche Punktzahl
average_passing_score	Durchschnittliche Punktzahl (bestanden)
total_registered	Durchschnittliche Punktzahl (nicht bestanden)
total_participants	Gesamtzahl der registrierten Benutzer
account_id	Gesamtteilnehmer

SCO-Details

Spalte	Beschreibung
sco_id	Sco-ID
sco_version	SCO-Version
sco_name	Name
sco_description	Beschreibung
sco_type	SCO-Typ
sco_int_type	Ganzzahltyp
is_content	Ist SCO ein Material-SCO?
url	URL
parent_name	Name des übergeordneten SCO
parent_sco_id	SCO-ID des übergeordneten SCO
parent_type	Typ des übergeordneten SCO
date_sco_created	Erstellungsdatum
date_sco_modified	Änderungsdatum
sco_start_date	Anfangsdatum
sco_end_date	Enddatum
version_start_date	Startdatum der Version
version_end_date	Enddatum der Version
sco_tag_id	Tag-ID
passing_score	Punktzahl (bestanden)
max_possible_score	Höchst mögliche Punktzahl
linked_sco_id	ID eines verknüpften SCO
linked_type	Typ eines verknüpften SCO
owner_user_id	Benutzer-ID des Eigentümers
storage_bytes_kb	Speicherbyte in Kilobyte
account_id	Benutzerkonto-ID

Aktivitäts-Fakt

Spalte	Beschreibung
dim_activity_details_activity_id	Aktivitäts-ID
score	Wertung
passed	Bestanden
completed	Abgeschlossen
peak_session_users	Benutzer mit Spitzenauslastung in Sitzung

Spalte	Beschreibung
number_correct	Zahl korrekt
number_incorrect	Zahl falsch
number_of_questions	Anzahl der Fragen
number_of_responses	Anzahl der Antworten
account_id	Benutzerkonto-ID

Aktivitäts-Details

Spalte	Beschreibung
activity_id	Aktivitäts-ID
dim_sco_details_sco_id	Sco-ID
dim_sco_details_sco_version	SCO-Version
dim_users_user_id	Benutzer-ID
dim_sco_details_parent_sco_id	ID der übergeordneten SCO
score	Wertung
passed	Bestanden
completed	Abgeschlossen
activity_type	Aktivitätstyp
role	Rolle
date_activity_started	Startdatum
date_activity_finished	Enddatum
dim_cost_center_id	ID der Kostenstelle
cost_center_audit_id	Audit-ID
session_start_date	Startdatum Sitzung
session_end_date	Enddatum Sitzung
attendance_activity	Gibt es Teilnehmeraktivität?
session_id	Sitzungs-ID
account_id	Benutzerkonto-ID

Studienplan - Einstufungstests

Spalte	Beschreibung
dim_sco_details_curriculum_sco_id	Studienplan-ID
dim_sco_details_curriculum_sco_version	Studienplanversion
test_out_subject_sco_id	Thema-SCO-ID
test_out_target_sco_id	Ziel-SCO-ID
test_out_type	Einstufungstyp

Spalte	Beschreibung
account_id	Benutzerkonto-ID

Voraussetzung für Studienplan

Spalte	Beschreibung
dim_sco_details_curriculum_sco_id	Studienplan-ID
dim_sco_details_curriculum_sco_version	Studienplanversion
pre_requisite_subject_sco_id	Thema-SCO-ID
pre_requisite_target_sco_id	Ziel-SCO-ID
pre_requisite_type	Art der Voraussetzung
account_id	Benutzerkonto-ID

Anforderungen für Abschluss des Studienplans

Spalte	Beschreibung
dim_sco_details_curriculum_sco_id	Studienplan-ID
dim_sco_details_curriculum_sco_version	Studienplanversion
completion_subject_sco_id	Thema-SCO-ID
completion_target_sco_id	Ziel-SCO-ID
completion_requirement_type	Art der Abschlussanforderung
account_id	Benutzerkonto-ID

Folienansichten - Fakten

Spalte	Beschreibung
dim_slide_view_details_slide_view_id	Folienansichts-ID
dim_activity_details_activity_id	Aktivitäts-ID
slide_view_display_sequence	Anzeigereihenfolge
account_id	Benutzerkonto-ID

Folienansichten - Details

Spalte	Beschreibung
slide_view_id	Folienansichts-ID
date_slide_viewed	Datum der Anzeige der Folie
slide_name	Folienname
slide_description	Folienbeschreibung
account_id	Benutzerkonto-ID

Antworten - Fakten

Spalte	**Beschreibung**
dim_answer_details_answer_id	Antwort-ID
dim_activity_details_activity_id	Aktivitäts-ID
dim_question_details_question_id	Frage-ID
answer_display_sequence	Anzeigereihenfolge
answer_score	Wertung?
answer_correct	Ist richtig?
account_id	Benutzerkonto-ID

Antwortdetails

Spalte	**Beschreibung**
answer_id	Antwort-ID
date_answered	Datum der Antwort
response	Antwort
account_id	Benutzerkonto-ID

Frage-Fakt

Spalte	**Beschreibung**
dim_sco_details_sco_id	Sco-ID
dim_sco_details_sco_version	SCO-Version
dim_question_details_question_id	Frage-ID
number_correct	Anzahl der korrekten Antworten
number_incorrect	Anzahl der falschen Antworten
total_responses	Antworten insgesamt
high_score	Hohe Punktzahl
low_score	Niedrige Punktzahl
average_score	Durchschnittliche Punktzahl
account_id	Benutzerkonto-ID

Fragen - Details

Spalte	**Beschreibung**
question_id	Frage-ID
question_display_sequence	Anzeigereihenfolge
question_description	Beschreibung
question_type	Fragetyp

Spalte	Beschreibung
account_id	Benutzerkonto-ID

Antworten auf Fragen

Spalte	Beschreibung
dim_question_details_question_id	Frage-ID
response_display_sequence	Anzeigereihenfolge der Antworten
response_value	Wert
response_description	Beschreibung
account_id	Benutzerkonto-ID

Gruppen

Spalte	Beschreibung
group_id	Gruppen-ID
group_name	Gruppenname
group_description	Gruppenbeschreibung
group_type	Gruppentyp
account_id	Benutzerkonto-ID

Benutzergruppen

Spalte	Beschreibung
user_id	Benutzer-ID
group_id	Gruppen-ID
group_name	Gruppenname
account_id	Benutzerkonto-ID

Benutzer

Spalte	Beschreibung
user_id	Benutzer-ID
Login	Anmelden
first_name	Vorname
last_name	Nachname
email	E-Mail-Adresse
user_description	Benutzerbeschreibung
user_type	Benutzertyp
most_recent_session	Datum der letzten Sitzung

Spalte	Beschreibung
session_status	Status der Sitzung
manager_name	Verwaltername
disabled	Deaktiviert
account_id	Benutzerkonto-ID
custom_field_1	Wert für benutzerdefiniertes Feld 1
custom_field_2	Wert für benutzerdefiniertes Feld 2
custom_field_3	Wert für benutzerdefiniertes Feld 3
custom_field_4	Wert für benutzerdefiniertes Feld 4
custom_field_5	Wert für benutzerdefiniertes Feld 5
custom_field_6	Wert für benutzerdefiniertes Feld 6
custom_field_7	Wert für benutzerdefiniertes Feld 7
custom_field_8	Wert für benutzerdefiniertes Feld 8
custom_field_9	Wert für benutzerdefiniertes Feld 9
custom_field_10	Wert für benutzerdefiniertes Feld 10

Namen benutzerdefinierter Felder

Spalte	Beschreibung
dim_column_name	Name der Spalte des benutzerdefinierten Feldes
custom_field_name	Name des benutzerdefinierten Feldes
account_id	Benutzerkonto-ID

Kostenstellen

Spalte	Beschreibung
cost_center_id	ID der Kostenstelle
cost_center_name	Name der Kostenstelle
cost_center_description	Beschreibung der Kostenstelle

Erstellen von benutzerdefinierten Berichten aus älteren Datenbankansichten

Hinweis: *Acrobat Connect Pro-Server 7 enthält Star-Schemaansichten, die Sie abfragen können, um benutzerdefinierte Berichte zu erstellen. Die älteren Datenbankansichten werden noch unterstützt, jedoch sind die Star-Schemaansichten standardisierter und robuster.*

Acrobat Connect Pro speichert Informationen zu Benutzern, Materialien, Kursen und Meetings in einer Datenbank. Die Benutzeraktivität füllt die Datenbank mit Daten. Mit Werkzeugen wie Adobe® ColdFusion® Studio und Business Objects Crystal Reports können Sie die Datenbank abfragen und die Daten anzeigen. Sie können auch SQL-basierte Werkzeuge wie SQL Query Analyzer verwenden.

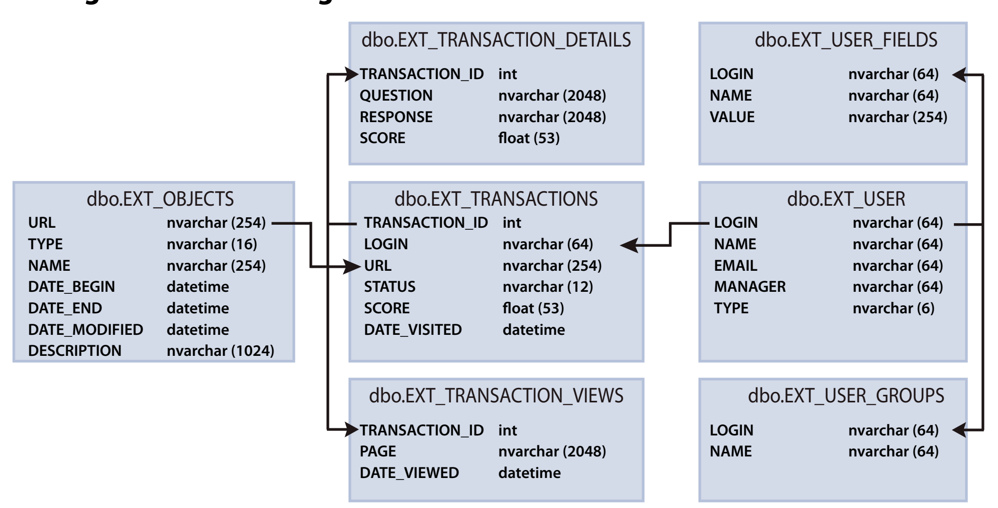
Die folgenden Acrobat Connect Pro-Anwendungen können Daten in Berichte ausgeben:

Acrobat Connect Pro Meeting Meetingteilnehmer, Meetingdauer und Meetingmaterialien

Adobe Presenter Materialansichten, Folienansichten und Präsentationsansichten

Acrobat Connect Pro Schulung Informationen zur Kursverwaltung wie Statistiken zu den Kursteilnehmern, Statistiken zur Materialanzeige und Quizergebnisse

Anzeigen von Beziehungen zwischen Datenbankansichten



Die Pfeile geben die Objektbeziehungen zwischen den sieben Berichtsansichten an.

***Hinweis:** Die folgenden Ansichten und Vorgänge werden nicht unterstützt: Ansichten, die in diesem Dokument nicht angegeben sind, das Bearbeiten von Ansichten, die in diesem Dokument angegeben sind oder der direkte Zugriff auf das zugrunde liegende Datenbankschema.*

❖ Verwenden Sie ein mit Ihrer Datenbank verbundenes Diagrammwerkzeug, um die Beziehungen zwischen den Datenbankansichten anzuzeigen.

EXT_TRANSACTIONS

Jedes Mal, wenn ein Benutzer mit einem Objekt interagiert, wird eine eindeutige Transaktions-ID erzeugt. Die Ansicht EXT_TRANSACTIONS gibt die in der folgenden Tabelle gelisteten Daten zurück:

Spalte	Datentyp	Beschreibung
TRANSACTION_ID	INT	Eindeutige ID für diese Transaktion
LOGIN	NVARCHAR	Name des Benutzers, der diese Transaktion ausgeführt hat
URL	NVARCHAR	Objekt, mit dem der Benutzer interagiert hat
STATUS	NVARCHAR	Statusmöglichkeiten: bestanden, nicht bestanden, abgeschlossen oder in Bearbeitung
SCORE	FLOAT	Punktzahl des Benutzers
DATE_VISITED	DATETIME	Datum, an dem die Transaktion stattfand oder angezeigt wurde

Beispielabfrage und -daten Die folgende Abfrage gibt die in der folgenden Tabelle aufgelisteten Daten zurück:

```
select * from ext_transactions where url = '/p63725398/' order by login, date_visited asc;
```

TRANSACTION_ID	LOGIN	URL	STATUS	SCORE	DATE_VISITED
10687	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10688	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10693	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:58:23.920
10714	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:09:20.810
10698	test2-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:00:49.483
10723	test3-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:11:32.153
10729	test3-lnagaraj@test.enang.com	/p63725398/	completed	20.0	2006-12-15 01:12:09.700

Abfragehinweise Die Ansicht EXT_TRANSACTIONS gibt alle vorhandenen Transaktionen für einen gegebenen Benutzer und eine gegebene Schulungssitzung zurück. Um die letzte Transaktion anzuzeigen, aktivieren Sie den maximalen Wert für DATE_VISITED.

Sie können die Felder STATUS und URL filtern, um eine Liste der für eine bestimmte Schulungssitzung in Frage kommenden Benutzer anzuzeigen. Beispielsweise:

```
select * from ext_transactions where url = '/p31102136/' and status = 'user-passed' order by
login, date_visited asc;
```

Daten generieren Benutzeraktionen, die Daten in dieser Ansicht generieren:

- Bei einem Meeting anwesend sein
- Material anzeigen
- An einer Schulungssitzung (Kurs oder Studienplan) teilnehmen

Ausgeschlossene Daten •Zertifikatnummer: ist in der Datenbank nicht vorhanden.

- Max. Punktzahl: häufig nicht verfügbar.

EXT_TRANSACTIONS_VIEWS

Die Ansicht EXT_TRANSACTIONS_VIEWS ruft Daten zu den Folien oder Seiten ab, die Benutzer anzeigen.

Spalte	Datentyp	Beschreibung
TRANSACTION_ID	INT	Eindeutige ID für diese Transaktion (kann mit TRANSACTION_DETAILS verbunden werden, um nach URL zusammengefasst zu werden).
PAGE	NVARCHAR	Nummer der angezeigten Folie oder Seite
DATE_VIEWED	DATETIME	Datum, an dem die Folie oder Seite angezeigt wurde

Beispielabfrage und -daten Die folgende Abfrage gibt die in der folgenden Tabelle aufgelisteten Daten zurück:

```
select * from ext_transaction_views where transaction_id = 10702 order by page asc;
```

TRANSACTION_ID	PAGE	DATE_VISITED
10702	0	2006-12-15 01:01:13.153
10702	2	2006-12-15 01:01:18.233
10702	2	2006-12-15 01:01:59.840
10702	3	2006-12-15 01:02:20.717

Daten generieren In dieser Ansicht werden jedes Mal Daten generiert, wenn ein Benutzer Material, oder einen Studienplan anzeigt.

EXT_USERS

In der Ansicht EXT_USERS werden die Benutzer und zugeordneten Profilattribute angezeigt:

Spalte	Datentyp	Beschreibung
LOGIN	NVARCHAR	Eindeutige Benutzer-ID
NAME	NVARCHAR	Eindeutiger Benutzername
EMAIL	NVARCHAR	Eindeutige E-Mail-Adresse.
MANAGER	NVARCHAR	Anmeldedaten des Verwalters. Der Verwalter ist in Breeze 5.1 immer auf NULL eingestellt.
TYPE	NVARCHAR	Benutzer oder Gast. In der Version 5.1 ist TYPE immer auf Benutzer eingestellt.

Beispielabfrage und -daten Die folgende Abfrage gibt die in der folgenden Tabelle aufgelisteten Daten zurück:

```
select * from ext_users;
```

LOGIN	NAME	EMAIL	MANAGER	TYPE
test4-lnagaraj@test.enang.com	test4 laxmi	test4-lnagaraj@test.enang.com	NULL	user
test7-lnagaraj@test.enang.com	TEST7 laxmi	test7-lnagaraj@test.enang.com	NULL	user

Daten generieren Daten werden in dieser Ansicht aktualisiert, wenn ein Gast oder Benutzer erstellt, aktualisiert oder gelöscht wird.

Ausgeschlossene Daten •Kennwort: nicht als einfacher Text gespeichert.

- Zeitzone und Sprache: nicht in einer einfach lesbaren Form verfügbar. PST (Pacific Standard Time) wird z. B. durch 323 dargestellt.
- Schnelle Anmeldung: zu ressourcenintensiv, um berechnet zu werden. Verwenden Sie stattdessen eine Abfrage `max(date_visited)` aus der Ansicht EXT_TRANSACTIONS, um die Daten abzurufen.
- Aktive Sitzung: Daten aus der Ansicht EXT_TRANSACTIONS. Verwenden Sie stattdessen eine Abfrage `STATUS='IN-PROGRESS'`, um die Daten abzurufen.
- Gelöschte Benutzer werden in der Ansicht EXT_USERS nicht aufgeführt. Gelöschte Benutzer werden in der Ansicht EXT_TRANSACTIONS weiterhin aufgeführt.
- Daten zu Gruppen sind in dieser Ansicht nicht aufgeführt.
- Daten in neuen und vordefinierten benutzerdefinierten Feldern. Diese Informationen sind für alle Benutzer in der Ansicht EXT_USER_FIELDS verfügbar.

EXT_USER_FIELDS

In der Ansicht EXT_USER_FIELDS werden neue und vordefinierte benutzerdefinierte Felder für einen spezifischen Benutzer aufgeführt. Darüber hinaus werden benutzerdefinierte Felder für Benutzer aufgeführt, die zu Gästen konvertiert wurden.

Spalte	Datentyp	Beschreibung
LOGIN	NVARCHAR	Eindeutige Benutzer-ID
NAME	NVARCHAR	Feldname wie Telefefonnummer
VALUE	NVARCHAR	Feldwert wie 415.555.1212

Beispielabfrage und -daten Die folgende Abfrage gibt die in der folgenden Tabelle aufgelisteten Daten zurück:

```
select * from ext_user_fields where login = 'test4-lnagaraj@test.enang.com';
```

LOGIN	NAME	VALUE
test4-lnagaraj@test.enang.com	{email}	test4-lnagaraj@test.enang.com
test4-lnagaraj@test.enang.com	{first-name}	test4
test4-lnagaraj@test.enang.com	{last-name}	laxmi
test4-lnagaraj@test.enang.com	{x-job-title}	sw engr 4
test4-lnagaraj@test.enang.com	{x-direct-phone}	NULL
test4-lnagaraj@test.enang.com	{x-direct-phone-key}	NULL
test4-lnagaraj@test.enang.com	SSN	777

Daten generieren Aktionen, die Daten in dieser Ansicht generieren: hinzufügen, erstellen, neue oder vordefinierte benutzerdefinierte Felder für einen oder mehrere Benutzer aktualisieren

EXT_USER_GROUPS

In der Ansicht EXT_USER_GROUPS werden alle Daten zu Gruppen und zugeordneten Gruppenmitgliedern aufgeführt. Die Ansicht EXT_USER_GROUPS gibt die in der folgenden Tabelle gelisteten Daten zurück:

Spalte	Datentyp	Beschreibung
LOGIN	NVARCHAR	Name des Benutzers
NAME	NVARCHAR	Name der Gruppe

Beispielabfrage und -daten Die folgende Abfrage gibt die in der folgenden Tabelle aufgelisteten Daten zurück:

```
select * from ext_user_groups where login = 'lnagaraj@adobe.com';
```

LOGIN	NAME
lnagaraj@adobe.com	{admins}
lnagaraj@adobe.com	{Autoren}
lnagaraj@adobe.com	{everyone}
lnagaraj@adobe.com	Laxmi Nagarajan

Abfragehinweise Das Verschachteln mehrere Gruppen wird in der Version 5.1 und höher unterstützt. Beispiel: Wenn Gruppe A Gruppe B enthält und Sie sich in Gruppe B befinden, werden Sie als Mitglied von A aufgeführt.

Integrierte Gruppen wie die Gruppe „Administratoren“ verwenden Codenamen im Schema. Siehe die folgende SQL-Abfrage: `SELECT * FROM EXT_USER_GROUPS where group='{admins}`. Mit dem Codenamen lassen sich integrierte Gruppen von benutzerdefinierten Gruppen unterscheiden.

Daten generieren Benutzeraktionen, die Daten in dieser Ansicht generieren:

- Gruppen erstellen, aktualisieren oder löschen
- Gruppenmitgliedschaft ändern

EXT_OBJECTS

In der Ansicht EXT_OBJECTS werden alle Systemobjekte (Meetings, Materialien, Kurse usw.) und ihre Attribute aufgeführt.

Spalte	Datentyp	Beschreibung
URL	NVARCHAR	Eindeutiger Bezeichner für das Objekt
TYPE	NVARCHAR	Präsentation, Kurs, FLV-Datei, SWF-Datei, Bild, Archiv, Meeting, Studienplan, Ordner oder Veranstaltung
NAME	NVARCHAR	Objektname wie in der Materialliste enthalten
DATE_BEGIN	DATETIME	Datum, an dem der Beginn des Objekts geplant ist
DATE_END	DATETIME	Datum, an dem das Ende des Objekts geplant ist
DATE_MODIFIED	DATETIME	Datum, an dem das Objekt geändert wurde
DESCRIPTION	NVARCHAR	Übersichtinformationen zum Objekt, die beim Erstellen eines neuen Meetings, Materials, Kurses oder eines anderen Objekttyps eingegeben wurden

Beispielabfrage und -daten Die folgende SQL-Abfrage gibt die in der folgenden Tabelle aufgelisteten Daten zurück:

```
select * from ext_objects order by type asc;
```

URL	TYPE	NAME	DATE_BEGIN	DATE_END	DATE_MODIFIED	DESCRIPTION
/p79616987/	course	test api	2006-12-08 23:30:00.000	NULL	2006-12-08 23:36:55.483	NULL
/p47273753/	curriculum	test review curric	2006-12-14 21:00:00.000	NULL	2006-12-14 21:00:30.060	NULL
/tz1/	meeting	{default-template}	2006-12-12 19:15:00.000	2006-12-12 20:15:00.000	2006-12-12 19:25:07.750	Präsentation zu Release
/p59795005/	presentation	In-QUIZ-TEST1	NULL	NULL	2006-12-15 00:43:19.797	Meeting der Verwalter

Abfragehinweise Sie können alle Objekte eines bestimmten Typs abrufen, indem Sie das Feld TYPE filtern. Die folgenden SQL-Abfragefilter gelten beispielsweise für Kurse und Studienpläne:

```
select * from ext_objects where type in ('course', 'curriculum');
```

Mit der folgenden SQL-Abfrage können Sie eine Liste der verfügbaren Systemtypen zurückgeben:

```
select DISTINCT (type) from ext_objects;
```

Daten generieren Benutzeraktionen, die Daten in dieser Ansicht generieren:

- Meeting, Kurs oder Studienplan erstellen oder aktualisieren
- Materialien hochladen oder aktualisieren

Ausgeschlossene Daten •Dauer: zu deren Berechnung sie `date_end - date_begin` verwenden können

- Größe auf Festplatte: exponiert Geschäftsregeln bezüglich Kopien gegenüber Originalen
- Ordner-ID
- Gelöschte Objekte werden in der Ansicht EXT_OBJECTS nicht aufgeführt. Gelöschte Objekte werden in der Ansicht EXT_TRANSACTION aufgeführt.